

Secure Entry Client

NCP

SECURE COMMUNICATIONS



Secure Entry Client

(WIN32/64)
Version 9.0
Januar 2007

Mit Anhang zu Mobile Computing, Domänenanmeldung und NCP Services

Copyright

Alle Programme und das Handbuch wurden mit größter Sorgfalt erstellt und nach dem Stand der Technik auf Korrektheit überprüft. Alle Haftungsansprüche infolge direkter oder indirekter Fehler, oder Zerstörungen, die im Zusammenhang mit den Programmen stehen, sind ausdrücklich ausgeschlossen.

Die in diesem Handbuch enthaltene Information kann ohne Vorankündigung geändert werden und stellt keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Ohne ausdrückliche schriftliche Erlaubnis der NCP engineering GmbH darf kein Teil dieses Handbuchs für irgendwelche Zwecke oder in irgendeiner Form mit irgendwelchen Mitteln, elektronisch oder mechanisch, mittels Fotokopie, durch Aufzeichnung oder mit Informationsspeicherungs- und Informationswiedergewinnungssystemen reproduziert oder übertragen werden.

MS-DOS®, Windows®, Windows NT®, Microsoft Accelerator Pack®, Microsoft Internet Explorer® und Microsoft® sind entweder eingetragene Warenzeichen oder Warenzeichen der Microsoft Corporation in den USA und/oder anderen Ländern. Alle anderen genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

Gesamtherstellung dieses Handbuchs:

Michael Lösel

Dokumentation + Publikation

ml-service@t-online.de

Pirckheimerstr. 47

90408 Nürnberg

0172 / 82 58 238



Network
Communications
Products engineering GmbH
Dombühler Str.2
D-90449 Nürnberg
Tel.: 0911 / 99 68-0
Fax: 0911 / 99 68-299
internet [http:// www.ncp.de](http://www.ncp.de)

NCP Hotline

Die NCP Hotline begleitet Sie mit technischem Sachverstand von der Beratung und Projektierung zur Installation, zum firmenspezifischen Training, bis zum Support in Ihrem Anwendungsumfeld.

Für eine umfassende Betreuung der NCP-Produkte im täglichen Einsatz bietet NCP Support von Montag bis Freitag, von 8:00 bis 17:00, der per Fax oder E-Mail kostenlos erreichbar ist, via Telefon per Dienstleistungsauftrag (siehe unten).

Service-Verträge werden nach Produkt-Gruppen abgeschlossen und umfassen alle dazugehörigen Produkte. Detaillierte Auskünfte zu Service-Verträgen erteilen NCP-Mitarbeiter unter: 09 11 / 99 68-0

**Dienstleistungsauftrag
nach Aufwand**

Auch ohne Service-Vertrag können Sie Dienstleistungen von NCP in Anspruch nehmen. Allerdings nur in beschränktem Umfang und nach einer schriftlichen Auftragserteilung Ihrerseits. In diesem Falle werden die von NCP erbrachten Leistungen nach Aufwand in Rechnung gestellt.

**Software Downloads
und Auskünfte**

Software Downloads und Informationen sind unter der Homepage von NCP erhältlich:
<http://www.ncp.de>
FTP-Server: <ftp://ftp.ncp.de>

Inhalt

1. Produktübersicht	13
1.1 Zum Umgang mit diesem Handbuch	13
1.2 Secure Entry Client – universeller IPSec Client	14
1.3 Secure Entry Client	15
Technische Daten	16
1.4 Secure Entry CE Client	18
Technische Daten	18
2. Installation	21
2.1 Installationsvoraussetzungen	22
Betriebssystem	22
Zielsystem	22
Lokales System	22
ISDN-Adapter (ISDN)	22
Analoges Modem (Modem)	22
LAN-Adapter (LAN over IP)	23
xDSL-Modem (PPPoE)	23
xDSL (AVM - PPP over CAPI)	23
Multifunktionskarte (GPRS/UMTS)	23
WLAN-Adapter (WLAN)	24
Automatische Medienerkennung	24
Voraussetzungen für den Einsatz von Zertifikaten	25
TCP/IP	25
Chipkartenleser	25
Chipkartenleser (CT-API-konform)	25
Chipkarten	26
Soft-Zertifikate (PKCS#12)	26
Chipkarten oder Token (PKCS#11)	26
2.2 Installation der Client Software	27
Installation und Lizenzierung	27
Installation von CD	27
2.2.1 Standard-Installation	28
2.3 Assistent für die erste Konfiguration	34
2.4 Update und Deinstallation	36
2.5 Upgrade auf den Secure Enterprise Client	37
2.6 Projekt-Logo	37
3. Client Monitor	39
3.1 Die Oberfläche des Client Monitors	40
3.1.1 Bedien- und Anzeigefelder	40
3.1.2 Das Erscheinungsbild des Monitors	41
Modifikationen der Oberfläche	41
3.1.3 Anwahl über das Profil an das Zielsystem	42
3.1.4 Die Symbole des Monitors	43
3.1.5 Statusanzeigen	44

EAP-Authentisierung	44
Chipkartenleser	44
PIN-Status	45
Firewall	45
3.1.6 Symbole des Verbindungsaufbaus	46
Symbole der NAS-Einwahl	46
Symbole der VPN-Einwahl	46
4. Monitor-Bedienung	48
4.1 Verbindung	49
4.1.1 Verbinden	50
4.1.2 Trennen	50
4.1.3 HotSpot-Anmeldung	50
4.1.4 Multifunktionskarte	51
Netzsuche	51
GPRS / UMTS aktivieren	52
SIM PIN eingeben	52
SIM PIN ändern	52
PUK Eingabe	53
4.1.5 Verbindungs-Informationen	53
Verbindungszeit	54
Timeout	54
Richtung	54
Durchsatz	54
Multilink	54
Verbindungsmedium	54
Kompression	54
Verschlüsselung	54
Schlüsselaustausch	55
Rx und Tx Bytes	55
4.1.6 Verfügbare Verbindungsarten	55
4.1.7 Zertifikate	56
Aussteller-Zertifikat anzeigen	56
Benutzer-Zertifikat anzeigen	57
Eingehendes Zertifikat anzeigen	57
CA-Zertifikate anzeigen	58
Anzeige und Auswertung von Zertifikats-Erweiterungen	58
Anzeige der Erweiterungen (Extensions)	59
Auswertung der Erweiterungen (Extensions)	60
4.1.8 PIN eingeben	61
Sicherung der PIN-Benutzung	62
4.1.9 PIN zurücksetzen	62
PIN-Status im Client Monitor	62
PIN-Eingabezwang nach Abmeldung oder Sleep-Mode	62
Anzeige der Meldungen des ACE-Servers für RSA-Token	62
4.1.10 PIN ändern	63
4.1.11 Verbindungssteuerung Statistik	64
4.1.12 Sperre aufheben	64
4.1.13 Beenden (des Monitors)	65

4.2	Konfiguration	66
4.2.1	Profil-Einstellungen	67
	Die Einträge der Profil-Einstellungen	67
4.2.2	Firewall-Einstellungen	70
	Eigenschaften der Firewall	71
	Konfiguration der Firewall-Einstellungen	71
	Konfigurationsfeld Grundeinstellungen	72
	Firewall deaktiviert	72
	Gesperrte Grundeinstellung (empfohlen)	72
	Offene Grundeinstellung	72
	Konfigurationsfeld Firewall-Regeln	73
	Erstellen einer Firewall-Regel	73
	Firewall-Regel / Allgemein	74
	Firewall-Regel / Lokal	76
	Firewall-Regel / Remote	77
	Firewall-Regel / Anwendungen	79
	Konfigurationsfeld Bekannte Netze	80
	Automatische Erkennung der bekannten Netze	81
	Friendly Net Detection mittels TLS	81
	Konfigurationsfeld Optionen	82
	Konfigurationsfeld Protokollierung	84
4.2.3	WLAN-Einstellungen	85
	Integrierte WLAN-Konfiguration für Windows 2000/XP	85
	WLAN-Automatik	85
	Netzsuche	85
	WLAN-Profile	86
	Statistik	88
4.2.4	Amtsholung	89
4.2.5	Zertifikate Konfiguration	90
	Benutzer-Zertifikat	91
	Zertifikat	91
	Chipkartenleser	92
	Port	92
	Auswahl Zertifikat	92
	PKCS#12-Dateiname	93
	PKCS#11-Modul	93
	Kein Verbindungsabbau bei gezogener Chipkarte	94
	PIN-Abfrage bei jedem Verbindungsaufbau	94
	PIN-Richtlinie	95
	Minimale Anzahl der Zeichen	95
	Weitere Richtlinien	95
	Zertifikatsverlängerung	95
4.2.6	Verbindungssteuerung Konfiguration	96
	Externe Anwendungen	96
	Überwachung	97
4.2.7	EAP-Optionen	98
4.2.8	Logon Optionen	99
	Anmelden	99
	Abmelden	100

Externe Anwendungen	100
Optionen	101
4.2.9 Konfigurations-Sperren	102
Allgemein Konfigurations-Sperren	102
Profile Konfigurations-Sperren	103
Allgemeine Rechte	103
Sichtbare Parameterfelder der Profile	103
4.2.10 Profile importieren	103
4.2.11 HotSpot	104
4.2.12 Profil-Sicherung	104
Erstellen	104
Wiederherstellen	104
4.3 Log	105
4.4 Fenster	107
4.4.1 Profilauswahl anzeigen	107
4.4.2 Buttonleiste anzeigen	108
4.4.3 Statistik anzeigen	108
4.4.4 WLAN-Status anzeigen	108
4.4.5 Immer im Vordergrund	109
4.4.6 Autostart	109
4.4.7 Beim Schließen minimieren	109
4.4.8 Nach Verbindungsaufbau minimieren	110
4.4.9 Sprache	110
4.5 Hilfe	111
4.5.1 Lizenzinfo und Aktivierung	111
4.5.2 Auf Updates prüfen	112
4.5.3 Info	112
4.6 Lizenzierung	113
4.6.1 Gültigkeitsdauer der Testversion	114
4.6.2 Software-Aktivierung	115
Online-Variante	116
Offline-Variante	118
4.7 Updates	125
4.7.1 Software-Updates	125
5. Konfigurationsparameter	127
5.1 Profil-Einstellungen	128
5.1.1 Grundeinstellungen	130
Profil-Name	131
Verbindungstyp	131
VPN zu IPsec-Gegenstelle	131
Internet-Verbindung ohne VPN	131
Verbindungsmedium	131
ISDN	131
Modem	131
LAN (over IP)	132
xDSL (PPPoE)	132
xDSL (AVM - PPP over CAPI)	132
GPRS / UMTS	132

	PPTP	132
	WLAN	133
	Ext. Dialer	133
	Automatische Medienerkennung	134
	Profil für automatische Medienerkennung verwenden	134
	Dieses Profil nach jedem Neustart des Systems verwenden	135
	Benutze Microsoft DFÜ-Dialer	135
5.1.2	Netzeinwahl	136
	Benutzername	137
	Passwort	137
	Passwort speichern	137
	Rufnummer (Ziel)	137
	Alternative Rufnummern	138
	Script-Datei	138
5.1.3	HTTP-Anmeldung	139
	Benutzername HTTP-Anmeldung	140
	Passwort HTTP-Anmeldung	140
	Passwort speichern HTTP-Anmeldung	140
	HTTP Authentisierungs-Script HTTP-Anmeldung	140
5.1.4	Modem	141
	Modem	142
	Anschluss	142
	Baudrate	142
	Com Port freigeben	142
	Modem Init. String	143
	Dial Prefix	143
	APN	143
	SIM PIN	143
5.1.5	Line Management	144
	Verbindungsaufbau	145
	Timeout	145
	Voice over IP (VoIP) priorisieren	146
	Dynamische Linkzuschaltung (Nur für ISDN)	146
	Schwellwert für Linkzuschaltung (Nur für ISDN)	146
	EAP-Authentisierung	147
	HTTP-Authentisierung	147
5.1.6	IPSec-Einstellungen	148
	Gateway	149
	IKE-Richtlinie	149
	IPSec-Richtlinie	150
	Exch. Mode	150
	PFS-Gruppe	150
	Richtlinien-Gültigkeit	151
	Dauer	151
	Richtlinien-Editor	151
	IKE-Richtlinie (editieren)	152
	Name IKE-Richtlinie	153
	Authentisierung IKE-Richtlinie	153
	Verschlüsselung IKE-Richtlinie	153

Hash IKE-Richtlinie	153
DH-Gruppe IKE-Richtlinie	153
IPSec-Richtlinie (editieren)	154
Name IPSec-Richtlinie	154
Protokoll IPSec-Richtlinie	154
Transformation (ESP) IPSec-Richtlinie	154
Transformation (Comp) IPSec-Richtlinie	154
Authentisierung IPSec-Richtlinie	154
5.1.7 Erweiterte IPSec-Optionen	155
IP-Kompression (LZS) verwenden	156
DPD (Dead Peer Detection) deaktivieren	156
UDP-Encapsulation verwenden	156
5.1.8 Identität	157
Typ Identität	158
ID Identität	158
Pre-shared Key verwenden	158
Extended Authentication (XAUTH) verwenden	158
Benutzername Identität	159
Passwort Identität	159
Zugangsdaten aus Konfiguration verwenden	159
5.1.9 IP-Adressen-Zuweisung	160
IKE Config Mode verwenden	161
Lokale IP-Adresse verwenden	161
IP-Adresse manuell vergeben	161
DNS/WINS	161
DNS-Server	161
WINS-Server	161
Domain Name	161
5.1.10 VPN IP-Netze	162
Netzwerk-Adressen VPN IP-Netze	163
Subnet-Masken	163
Auch lokale Netze im Tunnel weiterleiten	163
5.1.11 Zertifikats-Überprüfung	164
Benutzer des eingehenden Zertifikats	165
Aussteller des eingehenden Zertifikats	165
Fingerprint des Aussteller-Zertifikats	166
SHA1 Fingerprint verwenden	166
Weitere Zertifikats-Überprüfungen	166
5.1.12 Link Firewall	169
Stateful Inspection aktivieren	170
Ausschließlich Kommunikation im Tunnel zulassen	170
NetBIOS über IP zulassen	170
Bei Verwendung des Microsoft DFÜ-Dialers ausschließlich Kommunikation im Tunnel zulassen	170
6. Verbindungsaufbau	171
Verbindungsaufbau zum Zielsystem	171
Automatischer Verbindungsaufbau:	171
Manueller Verbindungsaufbau:	171

Wechselnder Verbindungsaufbau:	171
Verbinden	171
Client Logon	172
Passwörter und Benutzernamen	173
Passwort für NAS-Einwahl	173
Benutzername und Passwort für Extended Authentication	174
Verbindungsabbruch und Fehler	175
Trennen	175
Trennen und Beenden des Monitors	176
7. Beispiele und Erklärungen	177
7.1 IP-Funktionen	178
7.1.1 Geräte eines IP-Netzwerks	178
7.1.2 IP-Adress-Struktur	178
7.1.3 Netzmasken (Subnet Masks)	180
Beispiele	180
Standard-Masken	181
Reservierte Adressen	182
7.1.4 Zum Umgang mit IP-Adressen	182
7.2 Security	183
7.2.1 IPSec – Übersicht	183
IPSec – allgemeine Funktionsbeschreibung	183
7.2.2 Firewall-Einstellungen / Firewall Settings	185
7.2.3 SA-Verhandlung und Richtlinien / Policies	186
Phase 1 (Parameter der IKE-Richtlinie / IKE Policy):	186
Phase 2 (Parameter der IPSec-Richtlinie / IPSec Policy):	186
Kontrollkanal und SA-Verhandlung	187
IKE-Modi	188
7.2.4 IPSec Tunneling	190
Implementierte Algorithmen für Phase 1 und 2:	190
Unterstützte Authentisierung für Phase 1 (IKE-Richtlinie)	190
Unterstützte sym. Verschlüsselungsalgorithmen (Phase 1 + 2)	190
Unterstützte asym. Verschlüsselungsalgorithmen (Phase 1 + 2)	190
Unterstützte Hash-Algorithmen	191
Zusätzliche Unterstützung für Phase 2	191
Standard IKE-Vorschläge:	192
7.2.5 Zur weiteren Konfiguration	194
Basiskonfigurationen in Abhängigkeit vom IPSec Gateway	194
Gateway unterstützt nicht XAUTH	194
Gateway unterstützt IKE-Config Mode	194
Gateway unterstützt IKE-Config Mode nicht	195
7.2.6 IPSec Ports für Verbindungsaufbau und Datenverkehr	196
7.3 Zertifikats-Überprüfungen	197
7.3.1. Auswahl der CA-Zertifikate	197
7.3.2. Überprüfung der Zertifikats-Erweiterung	197
extendedKeyUsage	198
subjectKeyIdentifier / authorityKeyIdentifier	198
7.3.3. Überprüfung von Sperrlisten	198
7.4 Stateful Inspection-Technologie für die Firewall-Einstellungen	199

Abkürzungen und Begriffe	203
Index	217
 Anhang: Mobile Computing via GPRS/UMTS und	
Domänenanmeldung mit NCP Gina	A 1
Anhang: Secure Client Services	A23

1. Produktübersicht



Dieses Handbuch beschreibt Installation, Konfiguration, Leistungsumfang und Benutzeroberfläche des NCP Secure Entry Clients und seiner Komponenten.

Der NCP Secure Entry Client ist als Entry CE Client auch für das Betriebssystem Windows CE erhältlich.

Weitere Informationen zu Ausbaustufen und Produktvarianten erhalten Sie auf der NCP Website: <http://www.ncp.de>

1.1 Zum Umgang mit diesem Handbuch

Damit Sie sich in dieser Dokumentation schnell zurecht finden, ist im folgenden kurz ihr Aufbau dargestellt.

Das Handbuch ist in sechs größere Abschnitte untergliedert, die Step-by-Step oder dem Aufbau der grafischen Benutzeroberfläche folgend den jeweiligen Gegenstand beschreiben. Diesen Abschnitten folgen zwei Anhänge, die dem Verständnis und dem Auffinden von Fachtermini dienen.

1. Produktübersicht mit kurzer Beschreibung des Leistungsumfangs der Software
 2. Installationsanweisungen
 3. Beschreibung der grafischen Benutzeroberfläche,
 4. sowie der Konfigurationsmöglichkeiten
 5. Beschreibung der im Telefonbuch aufgelisteten Parameter
 6. Beschreibung eines Verbindungsaufbaus
 7. Beispiele und Erklärungen, insbesondere zu IPSec
- Anhänge mit einem Glossar (Abkürzungen und Begriffe) und einem Index

Querverweise sind im Text in Klammern gesetzt und geben die Verweisstelle mit dem Titel, bzw. nach einem Komma, mit dem Untertitel an.



Texte, die am Seitenrand mit einem Ausrufezeichen markiert sind, sollten besonders beachtet werden.



Weiterführende Hilfestellungen können jederzeit über die kontextsensitive Online-Hilfe abgerufen werden.

1.2 Secure Entry Client – universeller IPSec Client

Der IPSec Client kann in beliebigen VPN-Umgebungen eingesetzt werden. Er kommuniziert auf der Basis des IPSec-Standards mit den Gateways verschiedenster Hersteller* und ist die Alternative zu der am Markt angebotenen, einheitlichen IPSec-Client-Technologie. Die Client Software emuliert einen Ethernet LAN-Adapter. Der IPSec Client verfügt über zusätzliche Leistungsmerkmale, die dem Anwender den Einstieg in eine ganzheitliche Remote Access VPN-Lösung ermöglichen.

Der IPSec Client bietet:

- ☒ Unterstützung aller gängigen Betriebssysteme
- ☒ Einwahl über alle Übertragungsnetze
- ☒ Kompatibilität mit den VPN-Gateways unterschiedlichster Hersteller
- ☒ Integrierte Personal Firewall für mehr Sicherheit
- ☒ Dialer-Schutz (keine Bedrohung durch 0190er- und 0900er-Dialer)
- ☒ Höhere Geschwindigkeit im ISDN (Kanalbündelung)
- ☒ Gebührenersparnis (Kosten- und Verbindungskontrolle)
- ☒ Bedienungskomfort (grafische Oberfläche)
- ☒ Zentrales Management**

*) Kompatibilitätsliste kann angefordert werden unter marketing@ncp.de

**) optional

1.3 Secure Entry Client

Der NCP Secure Entry Client kommuniziert mit VPN-Gateways unterschiedlichster Hersteller auf Basis des IPSec-Standards. Es handelt es sich dabei um eine Client-Software, die alternativ zu den am Markt angebotenen Software Clients im Umfeld von Firewalls und Routern eingesetzt werden kann. Der Secure Entry Client hebt sich durch seine Leistungsmerkmale und Software-Architektur gegenüber anderen IPSec-Clients ab.

Vorteile des Secure Entry Clients:

- ☐ Unterstützung aller gängigen Betriebssysteme (Windows 32, Windows CE und Linux*). Lieferbar als NCP Secure Entry Client (Win32), NCP Secure Entry CE Client und NCP Secure Entry Linux Client*) auf Anfrage
- ☐ Einwahl über alle öffentlichen Übertragungsnetze
- ☐ Kompatibilität mit nahezu allen marktgängigen VPN-Gateways
- ☐ Integrierte, intelligente Personal Firewall
- ☐ Schutz vor fremden Dialern (0190 und 0900)
- ☐ Dömañenanmeldung
- ☐ Extending Authentication (XAUTH)-Support zur Authentisierung mittels USER ID / Passwort und/oder OTP
- ☐ Internet Key Exchange Config Mode (IKE CFG) für eine dynamische Zuweisung von IP-Adresse, DNS Server, Windows Name Server und Domain Name
- ☐ Dead Peer Detection (DPD-Konfiguration bei Tunnel Failover). Benutzerkonfigurierbare Zeitintervalle bei DPD-Vorfällen zur flexibleren Kontrolle für die Wiederherstellung von VPN-Tunnel
- ☐ Unterstützung des Extensible Authentication Protocols (EAP) mit den Funktionen Transport Layer Security (TLS) und MD5 (User ID/Passwort) zur sicheren Authentisierung des Anwenders gegenüber Access Points und Switches
- ☐ Network Address Translation-Traversal (NAT-T) für die Kommunikation zwischen Client und Gateway über Netzwerkkomponenten, die NAT durchführen
- ☐ Intelligentes Verbindungs-Management zur Minimierung der Übertragungskosten und Erhöhung der Transparenz (Gebühren-Manager)
- ☐ Hohe Übertragungsgeschwindigkeit im ISDN durch Kanalbündelung
- ☐ Grafische Benutzeroberfläche

Der Secure Entry Client unterstützt, wie alle NCP Secure Communications-Produkte, den Einsatz digitaler Zertifikate in einer Public Key-Infrastruktur (PKI). Ein Upgrade auf die NCP Secure Enterprise-Lösung mit leistungsstarkem, zentralem Management ist optional möglich.

Technische Daten

■ LAN-Emulation

Ethernet-Adapter mit NDIS Interface

■ PC-Betriebssysteme

Windows 98se, Windows NT (V4.0 SP5), Windows 2000, Windows ME, Windows XP Prof.

■ Netzwerkprotokolle

- IP
- IPSec-VPN: Unterstützung von Pre-Shared-Key und Zertifikaten, Zentrale Konfiguration der IPSec-Proposals, d.h. das zentrale VPN Gateway bestimmt die Richtlinien (für IKE, IPSec-Phase 2) für den Secure Entry Client.
- IPSec nach RFC 2401-2409: Zur Optimierung in Remote Access-Umgebungen werden zusätzlich die Drafts (XAUTH, IKE-Config, DPD, NAT-T, IP-Comp) unterstützt (RFCs und Drafts siehe unten).
- EAP-MD5, EAP-TLS: Extensible Authentication Protocol, erweiterte Authentifikation gegenüber Switches und Access Points (Layer 2).

■ Verschlüsselung

- Triple DES (128, 192 Bit)
- Blowfish (128 Bit)
- AES (128, 192, 256 Bit)
- RSA (1024, 2048 Bit)
- Hash-Verfahren
- SHA1 (Secure Hash Algorithm 1)
- MD5 (Message Digit 5)

■ Personal Firewall

- IP-NAT Network Address Translation
- Stateful Inspection
- Applikations- und Verbindungsabhängige Filterregeln
- Protokoll-, Port und Adressenbezogene Filterregeln
- Friendly Net-Erkennung
- Automatische Hotspot-Anmeldung
- Umfangreiche Logging-Optionen

■ Filtering

IP Broadcasts, Netbios over IP

■ PKI

- Public Key-Infrastruktur nach X.509 v.3 Standard, Entrust (Entrust Ready)
- SmartCards: PKCS#11, TCOS 1.2 und 2.0+CardOS M4 (über CT-API oder PC/SC)
- Soft Zertifikate: PKCS#12
- PIN-Richtlinie: Administrative Vorgabe für die Eingabe beliebig komplexer PINs
- Revocation Lists: Überprüfung der CRL (Certificate Revocation List) und ARL (Authority Revocation List)
- Zertifikatskontrolle: Überprüfung und Hinweis der Gültigkeitsdauer eines Zertifikates

■ Einmal-Passwort (One Time Password)

Komfortable Eingabe durch Trennung von PIN und Passwort, (RSA-Ready)

■ DynDNS

Anwahl des zentralen VPN Gateways mit wechselnder öffentlicher IP-Adressen, Abfrage der aktuellen IP-Adresse über einen öffentlichen DynDNS-Server

■ IP Adress Allocation

DHCP Dynamic Host Control Protocol

■ Point-to-Point Protokolle

- PPP over ISDN
- PPP over GSM (V.110)
- PPP over PSTN (Modem)
- PPP over Ethernet (xDSL)
- PPP LCP Link Control Protocol
- PPP IPCP IP Control Protocol
- PPP MLP Multilink Protocol
- PPP Call Back Verhandlung im LLC
- PPP PAP Password Authentication Protocol
- PPP CHAP Challenge Handshake Authentication Protocol

■ Dialer

- NCP-Dialer
- Alternativ: Microsoft RAS-Dialer für ISP-Einwahl mittels Einwahl-Script

■ Verbindungsmanagement

Weitere Informationen erhalten Sie unter info@ncp.de

Short Hold, Timeout (zeit- und gebührengesteuert)

■ **Kanalbündelung im ISDN**

Dynamisch, frei konfigurierbarer Schwellwert

■ **Client Monitor**

Konfiguration des Telearbeitsplatzes, Verbindungssteuerung und -überwachung

■ **Connection Manager**

Für die internationale Einwahl. Unterstützt werden: Gric, Infonet, UUNet

1.4 Secure Entry CE Client

Technische Daten

■ **LAN-Adapter**

- Ethernet-Adapter mit NDIS Interface
- Wireless LAN-Adapter

■ **Betriebssysteme**

Mobiles Endgerät: Windows CE 3.0 (Handheld PC 2000, Pocket PC 2002), Windows CE.net 4.2 (Windows Mobile 2003 for Pocket PC)

Konfigurations-PC: Windows 98se/ NT 4.0 ab SP5/ 2000/XP

■ **Netzwerkprotokolle**

- IP
- IPSec-VPN: Unterstützung von Pre-Shared-Key und Zertifikaten, Zentrale Konfiguration der IPSec-Proposals, d.h. das zentrale VPN Gateway bestimmt die Richtlinien (für IKE, IPSec-Phase 2) für den Secure Entry Client.
- IPSec nach RFC 2401-2409: Zur Optimierung in Remote Access-Umgebungen werden zusätzlich die Drafts (XAUTH, IKE-Config, DPD, NAT-T, IP-Comp) unterstützt (RFCs und Drafts siehe unten).

■ Verschlüsselung

- Triple DES (128, 192 Bit)
- Blowfish (128 Bit)
- AES (128, 192, 256 Bit)
- RSA (1024, 2048 Bit)

■ Hash-Verfahren

- SHA1 (Secure Hash Algorithm 1)
- MD5 (Message Digit 5)

■ Firewall-Funktionalitäten

- IP-NAT Network Address Translation
- Schutz des PCs bei VPN-Connection gegenüber Zugriffen von anderen Systemen (LAN-Adapter-Schutz)

■ Filtering

- IP Broadcasts
- Netbios over IP

■ PKI

- Public Key-Infrastruktur nach X.509 v.3 Standard
- SmartCards: TCOS 1.2 und 2.0 + CardOS M4 (PC/SC)
- Soft Zertifikate: PKCS#12

■ IP Adress Allocation

DHCP Dynamic Host Control Protocol

■ Point-to-Point Protokolle

- PPP LCP Link Control Protocol
- PPP IPCP IP Control Protocol
- PPP CCP Compression Control Protocol
- PPP PAP Password Authentication Protocol
- PPP CHAP Challenge Handshake Authentication Protocol
- PPP ECP Encryption Control Protocol

■ Kompressionsverfahren

Stac

■ Verbindungsmanagement

Short Hold, Timeout (zeitgesteuert)

■ Client Monitor

- Konfiguration des PDAs erfolgt über den Client Monitor an einem Standard-PC
- Der “PDA Monitor” dient zur Statusanzeige und Zielwahl

■ Dialer

- NCP-Dialer
- Microsoft RAS-Dialer

■ Optionen:

- Zentrales NCP Secure Enterprise VPN/PKI Gateway
- Upgrade auf NCP Secure Enterprise Solution mit zentralem Management-Tool und High Availability Services

■ RFCs und Drafts

- RFC 2401 – Security Architecture for the Internet Protocol
- RFC 2403 – The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404 – The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2406 – IP Encapsulating Security Payload (ESP)
- RFC 2407 – The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 – Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 – The Internet Key Exchange (IKE)
- RFC 3947 – Negotiation of NAT – Traversal in IKE
- RFC 3498 – UDP Encapsulation of IPSEC ESP packets
- DRAFT – Draft-beaulieu-ike-xauth-05 (XAUTH)
- DRAFT – Draft-dukes-ike-mode-cfg-02 (IKECFG)
- DRAFT – Draft-ietf-ipsec-dpd-01 (DPD)
- DRAFT – Draft-ietf-ipsec-nat-t-ike-01 (NAT-T)
- DRAFT – Draft-ietf-ipsec-nat-t-ike-02 (NAT-T)
- DRAFT – Draft-ietf-ipsec-nat-t-ike-03 (NAT-T)
- DRAFT – Draft-ietf-ipsec-nat-t-ike-05 (NAT-T)
- DRAFT – Draft-ietf-ipsec-udp-encaps-06 (UDP-ENCAP)

2. Installation

Die Installation der Software für Windows-Systeme erfolgt komfortabel über Setup. Der Installationsablauf ist für alle Versionen des IPSec Clients identisch. Im folgenden ist die Installation für Windows 2000/XP und Vista beschrieben.



Bevor Sie die Software installieren, müssen, zur vollen Funktionsfähigkeit die Installationsvoraussetzungen, wie im folgenden Kapitel beschrieben, erfüllt sein.

2.1 Installationsvoraussetzungen

Betriebssystem

Die Software kann auf Computern (min. 128 MB RAM) mit den Betriebssystemen Microsoft Windows 2000, Windows XP oder Windows Vista installiert werden. Halten Sie für die Dauer der Installation unbedingt die Datenträger (CD oder Disketten) für das jeweils im Einsatz befindliche Betriebssystem bereit, um Daten für die Treiberdatenbank des Betriebssystems nachladen zu können!

Zielsystem

Die Parameter für das Zielsystem werden über die Profil-Einstellungen eingegeben. Entsprechend der möglichen Verbindungsarten des Clients muss das Zielsystem eine der folgenden Verbindungsarten unterstützen: ISDN, PSTN (analoges Modem), LAN over IP oder PPP over Ethernet.

Lokales System



Eines der folgenden Kommunikationsgeräte und der entsprechende Treiber muss auf dem Client-PC installiert sein.

■ ISDN-Adapter (ISDN)

Der ISDN-Adapter muss die ISDN CAPI 2.0 unterstützen. Wenn Sie PPP Multilink nutzen, kann die Software bis zu 8 ISDN B-Kanäle (je nach Kanalanzahl des Adapters) bündeln. Jeder ISDN-Adapter, der die ISDN-Schnittstelle CAPI 2.0 unterstützt, kann eingesetzt werden. (Die CAPI wird mit der Installation des Adapters eingerichtet.)

■ Analoges Modem (Modem)

Für die Kommunikation über Modem muss das Modem korrekt installiert sein, sowie Modem Init. String und COM-Port Definition zugewiesen sein. Das Modem muss den Hayes-Befehlssatz unterstützen.

Ebenso können Mobiltelefone für die Datenkommunikation genutzt werden, nachdem die zugehörige Software installiert wurde, die sich für den Client genauso darstellt wie ein analoges Modem. Als Schnittstelle zwischen Handy und PC kann die serielle Schnittstelle, die IR-Schnittstelle (Infrarot) oder Bluetooth genutzt werden. Je nach Übertragungsart (GSM, V.110, GPRS, UMTS oder HSCSD) muss die Gegenstelle über die entsprechende Einwahlplattform verfügen. Der in die Modemkonfiguration des

Secure Clients einzutragende Initialisierungs-String ist vom ISP oder dem Hersteller des Mobiltelefons zu beziehen.

■ LAN-Adapter (LAN over IP)

Um die Client-Software mit der Verbindungsart "LAN" in einem Local Area Network betreiben zu können, muss zusätzlich zum bereits installierten LAN-Adapter (Ethernet) kein weiterer Adapter installiert werden. Die Verbindung der LAN-Clients ins WAN stellt ein beliebiger Access Router her. Einzige Voraussetzung: IP-Verbindung zum Zielsystem muss möglich sein. Die VPN-Funktionalität liefert die Client Software.

■ xDSL-Modem (PPPoE)

Die Verbindungsart PPP over Ethernet setzt voraus, dass eine Ethernet-Karte installiert und darüber ein xDSL-Modem mit Splitter korrekt angeschlossen ist.

■ xDSL (AVM - PPP over CAPI)

Diese Verbindungsart kann gewählt werden, wenn eine AVM Fritz! DSL-Karte eingesetzt wird. Im Feld "Rufnummer (Ziel)" in der Gruppe "Netzeinwahl" können für die Verbindung über CAPI noch AVM-spezifische Initialisierungskommandos eingetragen werden. Unter Windows Betriebssystemen wird jedoch empfohlen den Standard "xDSL (PPPoE)" zu verwenden, da damit direkt über die Netzwerkschnittstelle mit der Karte kommuniziert wird.

Bei Verwendung der AVM Fritz! DSL-Karte wird keine separate zusätzliche Netzwerkkarte benötigt.

■ Multifunktionskarte (GPRS/UMTS)

Wird eine Multifunktionskarte für UMTS/GPRS/WLAN eingesetzt, so können mit der Client Software spezielle Features des Mobile Computings unter Einbeziehung der Karteneigenschaften genutzt werden (siehe - Handbuch-Anhang "Mobile Computing via GPRS/UMTS"). Aufgrund der direkten Unterstützung einer Multifunktionskarte durch den Secure Client kann die Installation einer Management-Software von der eingesetzten Karte entfallen. Die VPN-Verbindung wird unabhängig vom Microsoft DFÜ-Netzwerk über den integrierten NCP Dialer aufgebaut. Derzeit werden folgende Multifunktionskarten unterstützt:

- T-Mobile Multimedia NetCard
- Vodafone Mobile Connect Card
- KPN Mobile Connect Card
- T-Mobile DSL card 1800
- integrierte Karte des Lenovo Notebooks (Sierra Chipset)
- Vodafone EasyBox USB-Adapter für UMTS/GPRS

■ WLAN-Adapter (WLAN)

Der WLAN-Adapter wird mit der Verbindungsart “WLAN” betrieben. Im Monitormenü erscheint eigens der Menüpunkt “WLAN-Einstellungen”, worin die Zugangsdaten zum Funknetz in einem Profil hinterlegt werden können. Wird diese “WLAN-Konfiguration aktiviert”, so muss das Management-Tool der WLAN-Karte deaktiviert werden. (Alternativ kann auch das Management-Tool der WLAN-Karte genutzt werden, dann muss die WLAN-Konfiguration im Monitormenü deaktiviert werden.)

Wird die Verbindungsart WLAN für ein Zielsystem im Telefonbuch eingestellt, so wird unter dem grafischen Feld des Client-Monitors eine weitere Fläche eingeblendet, auf der die Feldstärke und das WLAN-Netz dargestellt werden.



Bitte beachten Sie zur Konfiguration der WLAN-Einstellungen die Beschreibung zum Parameter “Verbindungsart” im Handbuchabschnitt “Profile” und den Anhang “Mobile Computing”.

■ Automatische Medienerkennung

Werden wechselweise unterschiedliche Verbindungsarten genutzt, so erkennt der Client automatisch, welche Verbindungsarten aktuell zur Verfügung stehen und wählt davon die schnellste aus.

Auf Grundlage eines vorkonfigurierten Zielsystems wird automatisch die Verbindungsart erkannt und eingesetzt, die für den Client-PC aktuell zur Verfügung steht, wobei bei mehreren alternativen Übertragungswegen automatisch der schnellste gewählt wird. In einer Suchroutine ist die Priorisierung der Verbindungsarten in folgender Reihenfolge festgelegt: 1. LAN, 2. WLAN, 3. DSL, 4. UMTS/GPRS, 5. ISDN, 6. MODEM.

Die Konfiguration erfolgt mit der Verbindungsart “automatische Medienerkennung” im Telefonbuch unter “Zielsystem”. Alle für diesen Client-PC vorkonfigurierten Zielsysteme zum VPN Gateway des Firmennetzes können dieser automatischen Medienerkennung sofern gewünscht zugeordnet werden (über das Parameterfeld “Zielsystem” im Telefonbuch). Damit erübrigt sich die manuelle Auswahl eines Mediums (WLAN, UMTS, Netzwerk, DSL, ISDN, Modem) aus den Telefonbucheinträgen. Die Eingangsdaten für die Verbindung zum ISP werden für den Anwender transparent aus den vorhandenen Telefonbucheinträgen übernommen.



Beachten Sie dazu die Beschreibung zu “Profil-Einstellungen / Verbindungsart”.

Voraussetzungen für den Einsatz von Zertifikaten



Um mit der Security Software die Zertifizierung (X.509) nutzen, zu können, müssen folgende Voraussetzungen erfüllt sein:

■ TCP/IP

Das Netzwerk-Protokoll TCP/IP muss auf dem Rechner installiert sein.

■ Chipkartenleser

Wenn Sie die “Erweiterte Authentisierung” (Strong Authentication) mit Smart Cards nutzen wollen, muss ein Chipkartenleser an Ihr System angeschlossen sein. Die Client Software unterstützt automatisch alle Chipkartenleser, die PC/SC-konform sind. Diese Chipkartenleser werden nur in der Liste der Chipkartenleser aufgenommen, nachdem der Leser angeschlossen und die zugehörige Treiber-Software installiert wurde. Die Client Software erkennt dann den Chipkartenleser nach einem Boot-Vorgang automatisch. Erst dann kann der installierte Leser ausgewählt und genutzt werden. Dazu stellen Sie nach dem ersten Start des Monitors den Chipkartenleser ein unter “Konfiguration → Zertifikate”. Nachdem Sie die Smart Card in den Chipkartenleser gesteckt haben, können Sie Ihre PIN eingeben.

■ Chipkartenleser (CT-API-konform)

Wenn Sie einen CT-API-konformen Chipkartenleser nutzen, beachten Sie bitte folgendes:

- ☒ Mit der aktuellen Software werden Treiber für die Modelle Kobil B0/B1, Kobil KAAAN, SCM Swapsmart und SCM 1x0 (PIN Pad Reader) mitgeliefert. Diese Chipkartenleser können im Monitor unter “Konfiguration → Zertifikate” eingestellt werden. Sollte der Chipkartenleser mit den mitgelieferten Treibern nicht funktionieren oder ein anderer Chipkartenleser installiert sein, wenden Sie sich unbedingt an den Hersteller des Chipkartenlesers, bzw. konsultieren Sie die entsprechende Website bezüglich aktueller Hardware-Treiber, um den aktuellsten CT-API-Treiber zu erhalten und zu installieren. Nehmen Sie außerdem folgende Einstellung in der Client Software vor:
- ☒ Editieren Sie die Datei NCPPKI.CONF, befindlich im Installationsverzeichnis, indem Sie als "Modulname" den Namen des angeschlossenen Chipkartenlesers (xyz) eintragen und als DLLWIN95 bzw. DLLWINNT den Namen des installierten Treibers eintragen. Für die NT-basierenden Betriebssysteme Windows 2000 und Windows XP ist der Modulname DLLWINNT zu benutzen. (Der Standardname für CT-API-konforme Treiber ist CT32.DLL).



Wichtig: Nur die Treiber sind in der Liste sichtbar, die mit “visible = 1” auf sichtbar gesetzt wurden!

Modulname	= SCM Swapsmart (CT-API)	→ xyz
DLLWIN95	= scm20098.dll	→ ct32.dll
DLLWINNT	= scm200nt.dll	→ ct32.dll

- ☒ Nach einem Boot-Vorgang erscheint der von Ihnen eingetragene “Modulname” im Monitor-Menü unter “Konfiguration → Zertifikate → Chipkartenleser”. Selektieren Sie nun diesen Chipkartenleser.

■ Chipkarten

Folgende Chipkarten können direkt bei PC/SC- oder CT-API-Auswahl genutzt werden:

- Signtrust
- NetKey 2000
- TC Trust (CardOS M4)
- Telesec PKS SigG

■ Soft-Zertifikate (PKCS#12)

Statt einer Smart Card können auch Soft-Zertifikate genutzt werden.

■ Chipkarten oder Token (PKCS#11)

Mit der Software für die Smart Card oder den Token werden Treiber in Form einer PKCS#11-Bibliothek (DLL) mitgeliefert. Diese Treiber-Software muss zunächst installiert werden. Anschließend muss die Datei NCPPKI.CONF editiert werden.

- ☒ Editieren Sie die Datei NCPPKI.CONF, befindlich im Installationsverzeichnis, indem Sie als "Modulname" den Namen des angeschlossenen Lesers oder Tokens (xyz) eintragen. Als PKCS#11-DLL muss der Name der DLL eingegeben werden. Der zugehörige "Slotindex" ist herstellerabhängig (Standard = 0).



Wichtig: Nur die Treiber sind in der Liste sichtbar, die mit “visible = 1” auf sichtbar gesetzt wurden!

Modulname = xyz
PKCS#11-DLL = Name der DLL
Slotindex =

- ☒ Nach einem Boot-Vorgang erscheint der von Ihnen eingetragene “Modulname” im Monitor-Menü unter “Verbindung → Zertifikate → Konfiguration → Chipkartenleser”. Selektieren Sie nun diesen Chipkartenleser oder Token.

2.2 Installation der Client Software



Die vorliegende Version und künftige Versionen des Clients werden von der Qualitätssicherung nur noch für die Windows-Betriebssysteme Windows 2000, Windows XP und Windows Vista getestet. Für Windows NT sowie Windows 98 oder älter kann somit keine Gewähr mehr für die volle Funktionsfähigkeit der Client Software übernommen werden.



Sie können die Software in Form einer EXE-Datei als Download von der NCP- Internetseite unter www.ncp.de beziehen. Die Installation erfolgt für die Betriebssysteme Windows 2000/XP und Vista im Wesentlichen gleich.

Installation und Lizenzierung

Der NCP Secure Entry Client wird zunächst immer als Testversion installiert. Haben Sie eine Lizenz erworben, so können die Lizenzierungsdaten nach der Installation und einem Reboot im Monitor-Menü “Hilfe / Lizenzinfo und Aktivierung” eingegeben werden. Spätestens in den letzten 10 Tagen vor Ablauf der 30-tägigen Gültigkeitsdauer der Testversion werden Sie im Client-Monitor daran erinnert, dass eine Lizenzierung vorgenommen werden muss, wenn die Client Software weiter verwendet werden soll. Bitte beachten Sie zur Lizenzierung die Beschreibung im Handbuchabschnitt zum Monitor-Menüpunkt “Hilfe / Lizenzinfo und Aktivierung”.

Bei der Installation des NCP Secure Clients unter Windows XP und Windows Vista

Die Systemeigenschaften des Betriebssystems Windows XP sind bei Neueinrichtung restriktiv beschaffen. Sie sind standardmäßig so eingestellt, dass bei der Installation von Treiber-Software, die nicht von Microsoft lizenziert wurde, ein MS-spezifischer sogenannter “Windows-Logo-Test” durchgeführt wird, in dessen Folge das Betriebssystem davor warnt, die Treiber-Software zu installieren. Dem kann auf zwei Arten begegnet werden:

- ☒ Ändern Sie die restriktive Einstellung des Systems. Unter “System / Systemeigenschaften / Hardware / Geräte manager / Treibersignaturoptionen” ändern Sie das Vorgehen von Windows auf “Ignorieren - Software unabhängig von Zulassung installieren”!
- ☒ Nehmen Sie die obige Einstellungsänderung nicht vor, erscheint während des Setups nach dem Kopieren der Dateien eine Meldung, die vor der Installation des Client Adapters warnt – ignorieren Sie diese Meldung und klicken Sie auf “Installation fortsetzen”!

Installation von der CD



Nachdem Sie die CD in das Laufwerk Ihres Computers eingelegt haben, erscheint nach einigen Sekunden automatisch die Begrüßungsmaske auf Ihrem Monitor. Sie wählen aus, welches Produkt Sie installieren möchten und klicken anschließend auf “Installieren”. Das weitere Verfahren ist mit der Standard-Installation ab “Wählen der Setup-Sprache” identisch.

2.2.1 Standard-Installation

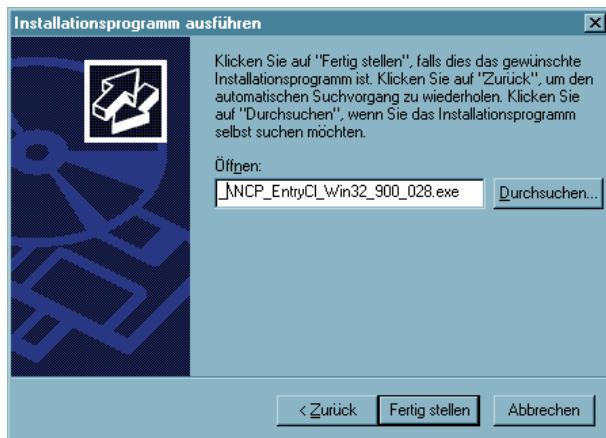
Die EXE-Datei, die Sie mit einem Download oder mit der CD erhalten haben, kopieren Sie auf die Festplatte des PCs. Der Dateiname der EXE-Datei beinhaltet Versions- und Build-Nummer der Software, z. B.:

`NCP_EntryCl_Win32_900_028.EXE`

Wählen Sie im Windows-Hauptmenu “Start / Einstellungen / Systemsteuerung”. In der Windows-Systemsteuerung wählen Sie “Software” oder “Neue Programme hinzufügen”. Klicken Sie dann auf den Button zum Installieren von CD oder Diskette.

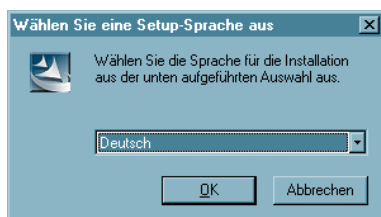


Wenn nebenstehendes Fenster erscheint klicken Sie auf “Weiter”.



Im daraufhin erscheinenden Fenster klicken Sie auf “Durchsuchen”, um die EXE-Datei Ihrer Software zu suchen.

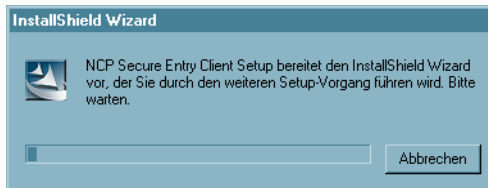
Wenn sie angezeigt wird, klicken Sie auf “Fertigstellen”.



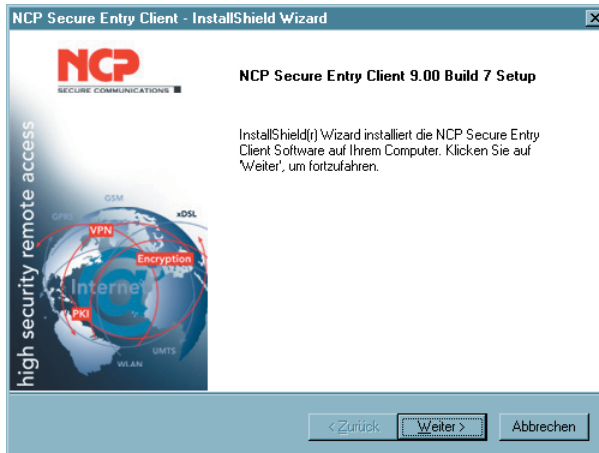
“Wählen der Setup-Sprache”

Im folgenden Fenster können Sie die Setup-Sprache auswählen. Klicken Sie danach auf “OK”.

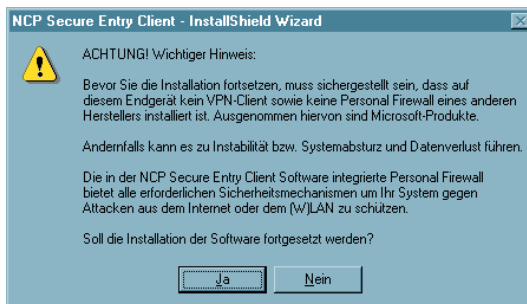
→ weiter nächste Seite



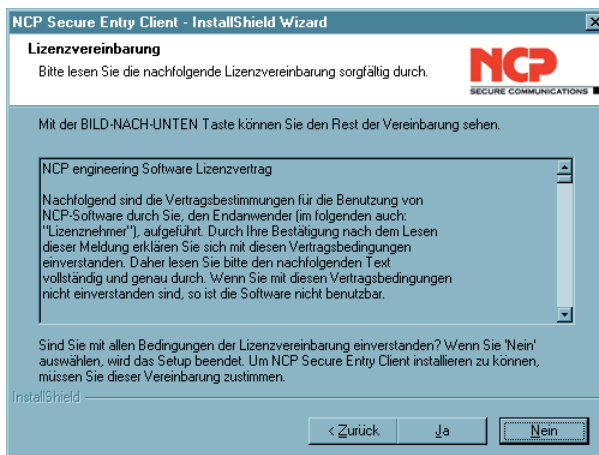
Anschließend bereitet das Setup-Programm den Install-Shield Assistenten vor, mit dessen Hilfe die Installation fortgesetzt wird.



Lesen Sie bitte die Hinweise im Willkommen-Fenster des Setup-Programms bevor Sie auf "Weiter" klicken.

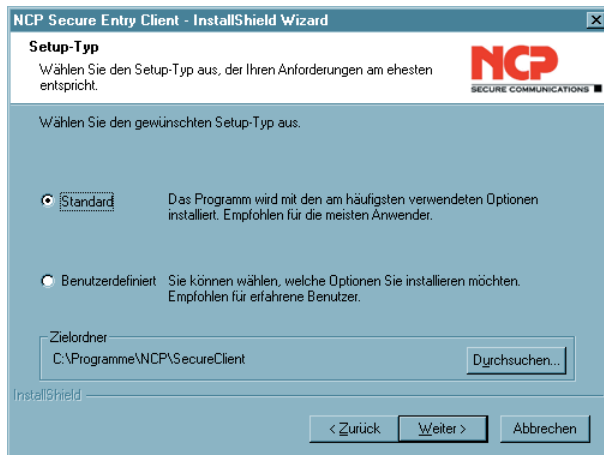


Bitte beachten Sie den nebenstehenden Hinweis und deaktivieren Sie VPN Client und Personal Firewall eines fremden Herstellers, um Instabilität oder Datenverlust zu vermeiden,

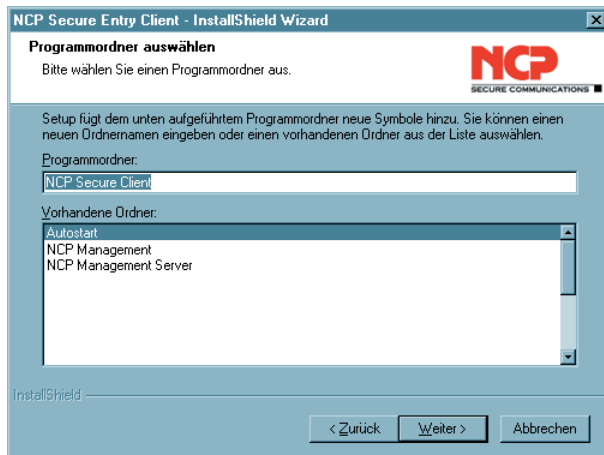
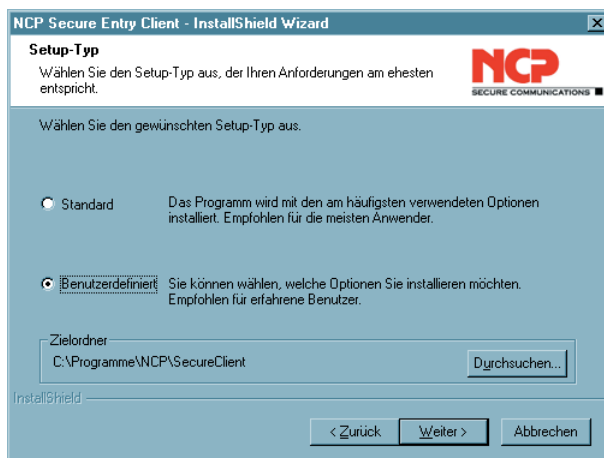


Anschließend werden die Lizenzbedingungen gezeigt. Stimmen Sie dem Vertrag mit "Ja" zu, sonst wird die Installation abgebrochen.

→ weiter nächste Seite



* Unter Windows Vista kann auch
 "Program Files\NCP\SecureClient" angezeigt werden.



Standard-Installationsverzeichnis* ist:
 Programme\NCP\SecureClient

Unabhängig von Standard- oder benutzerdefinierter Installation können Sie einen beliebigen Zielordner für die Software wählen, wenn Sie "Durchsuchen" anklicken. Dies ist insbesondere dann wichtig, wenn der Benutzer keine Rechte auf das System-Root-Verzeichnis hat.

Bei **Standard-Installation** ist das Setup mit diesem Fenster (links) abgeschlossen.

Nehmen Sie eine „**Benutzerdefinierte Installation**“ vor, so können Sie weitere Einstellungen vornehmen.

Im folgenden Fenster der "Benutzerdefinierten Installation" bestimmen Sie den Programmordner für die Client Software. (Standard ist "NCP Secure Entry Client").

→ weiter nächste Seite



Außerdem kann das Icon auf dem Desktop angezeigt werden.

Zu den weiteren Einstellungen bezüglich Ihres Gateways sind nähere Informationen von Ihrem Administrator oder Internet Service Provider nötig.



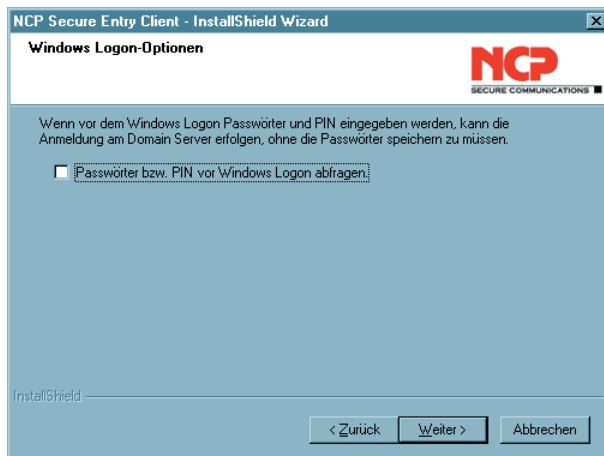
Mit DHCP (Dynamic Host Control Protocol) zu kommunizieren, bedeutet, dass Sie für jede Session automatisch eine IP-Adresse zugewiesen bekommen. In diesem Fall klicken Sie auf „IP-Adresse wird von Server vergeben“.

Wenn Sie die „IP-Adresse selbst festlegen“, geben Sie in diesem Fenster die IP-Adressen ein. Bitte beachten Sie: Ist bereits eine Netzwerkkarte mit Default Gateway installiert, so muß der Eintrag „Default Gateway“ hier gelöscht werden. Es darf nur eine Netzwerkkarte mit Default Gateway installiert sein. Die DNS-Adresse bitte nur eintragen, wenn Sie sie von Ihrem Provider oder Systemadministrator zur Verfügung gestellt bekommen haben.



Ende der benutzerdefinierten Installation!

→weiter nächste Seite



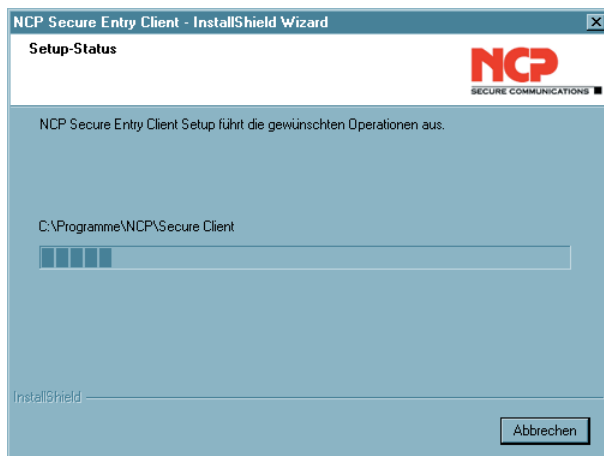
Sie können anschließend entscheiden, ob vor dem Windows-Logon an einer remote Domain die Verbindung zum Network Access Server aufgebaut werden soll. Für diesen Verbindungsaufbau müssen Sie gegebenenfalls die PIN für ihr Zertifikat und das (nicht gespeicherte) Passwort für die Client Software eingeben. Nachdem die Verbindung zum NAS hergestellt wurde, können Sie sich an die remote Domain anmelden. Diese Anmeldung erfolgt dann bereits verschlüsselt.



Bitte beachten Sie: Aktivieren Sie diese Option vor dem Windows Logon, so wird hiermit automatisch die NCP Gina installiert. Nur wenn die NCP Gina – wie in diesem Setup-Fnenter möglich – nach der Windows Gina installiert ist, können die Logon-Optionen auch genutzt werden. Diese Logon-Optionen können über das Monitormenü des Clients unter “Konfiguration” gesetzt werden.



Wird die Logon-Option hier nicht aktiviert, und soll sie jedoch zu einem späteren Zeitpunkt genutzt werden, so kann die NCP Gina nach diesem Setup mit dem Kommando `rwscmd / ginainstall` dauerhaft installiert werden. Beachten Sie dazu die Beschreibung “Secure Client Services” im Anhang dieses Handbuchs.



Danach werden die Dateien der Client Software eingespielt.

Anschließend werden die Netzwerkkomponenten installiert.

→ *weiter nächste Seite*

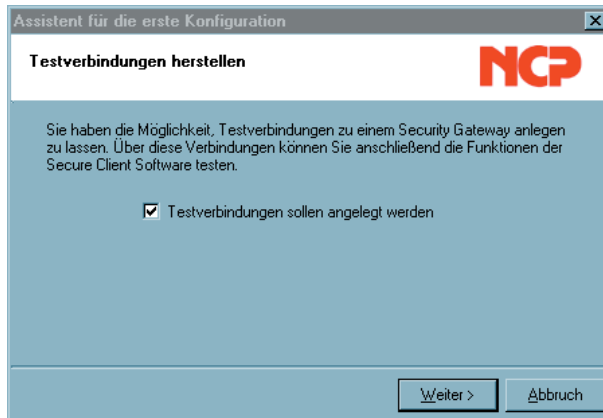


Damit ist die Installation der Client Software abgeschlossen. Die neuen Einstellungen werden erst wirksam, wenn Sie den Computer neu starten. Klicken Sie "Ja, Computer jetzt neu starten" und betätigen Sie den Button mit "Fertig stellen", um Ihr System zu booten.

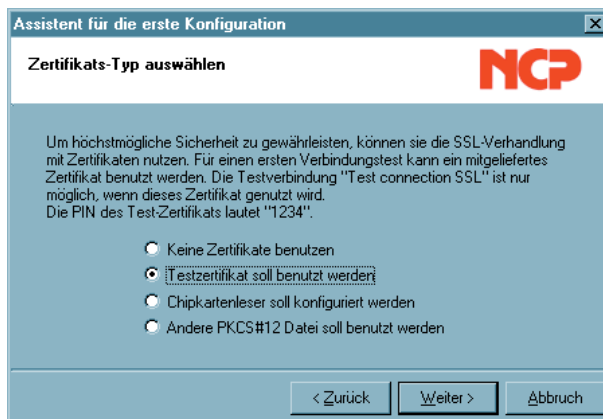
2.3 Assistent für die erste Konfiguration

Nachdem Sie die Software installiert haben und zum Abschluss der Installation den Rechner gebootet haben, wird der Client Monitor automatisch nach dem Booten geladen. Außerdem wird automatisch der “Assistent für die erste Konfiguration” gestartet, vorausgesetzt, Sie haben den Secure Client zum ersten Mal installiert oder das Telefonbuch (ncpphone.cfg) aus dem Installationsverzeichnis gelöscht.

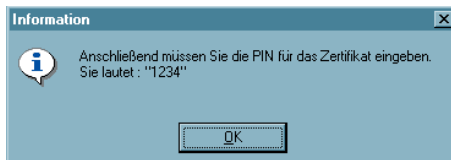
Wenn Sie keine Test-Verbindungen anlegen und den “Assistent für erste Konfiguration” abbrechen, erstellen Sie die ersten Telefonbucheinträge, wie im Handbuch unter “Client Monitor / Neuer Eintrag / Zielsystem” beschrieben.



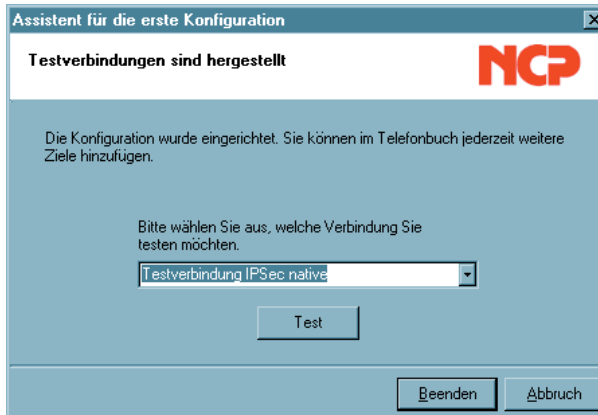
Nutzen Sie den “Assistent für erste Konfiguration”, so klicken Sie auf den Button “Weiter”. Dann legt der Assistent nach der Vorgabe Ihrer Daten ein Profil für eine IPSec-Testverbindung im Telefonbuch an. Dafür werden folgende Zugangsdaten automatisch gesetzt: VPN-Protokoll ist IPSec, der Tunnel-Endpunkt des Ziel-Gateways ist: 62.153.165.36, als XAUTH-Benutzername und XAUTH-Passwort wird “ncpipsecnative” eingetragen. Als Verbindungsart wird LAN genutzt. Soll eine Verbindung über einen ISP hergestellt werden, so müssen zuerst die Einwahl-Parameter in den Profil-Einstellungen der Testverbindung entsprechend konfiguriert werden.



Wenn Sie die Strong Security-Variante des Clients testen wollen, können Sie dafür ein mitgeliefertes Testzertifikat nutzen.



Die PIN für das Testzertifikat lautet "1234" und muss bei Verbindungsaufbau eingegeben werden.



Nachdem die Testkonfiguration angelegt wurde, kann sofort eine Test-Verbindung aufgebaut werden (sofern die Verbindung im LAN-Modus stattfindet.)

Klicken Sie dazu den Test-Button an.



Nach dem Verbindungsaufbau stellt sich die Oberfläche des Client-Monitors wie im linken Bild dar.

Soll die Testverbindung über eine andere Verbindungsart als LAN erfolgen, so beachten Sie bitte zur weitergehenden Konfiguration eines Profils die Beschreibungen unter "Client Monitor, Profil-Einstellungen" und "Konfigurationsparameter, IPSec-Einstellungen".



Zur Aktivierung der Software beachten Sie bitte den Abschnitt 4.6 Lizenzierung in diesem Handbuch.

2.4 Update und Deinstallation



Wenn bei der Installation eine ältere Version der Client Software gefunden wird, haben Sie die Möglichkeit, ein Update durchzuführen. Die Profil-Einstellungen, Zertifikate und die Verbindungssteuerung werden bei einem Update in der früher gemachten Konfiguration beibehalten. (Sollten noch andere Programme laufen, werden diese nun gestoppt.)

Um die Client Software zu entfernen, gehen Sie zu: “Start” → “Einstellungen” → “Systemsteuerung”. Klicken Sie nun auf “Software” und wählen Sie den Client aus der Liste. Klicken Sie dann auf den Button mit “Hinzufügen/Entfernen”. Das Uninstall Shield Programm löscht nun die Client Software von Ihrem PC.



Wichtig: Nachdem die Komponenten entfernt wurden, ist das Telefonbuch des Clients erhalten geblieben, so dass es für neuere Versionen des Secure Clients genutzt werden kann. Um die Dateien vollständig vom PC zu löschen, muss per Hand das komplette Installationsverzeichnis entfernt werden (Standard: \ncple).

2.5 Upgrade auf den Secure Enterprise Client

Ein Upgrade von einem Secure Entry Client auf einen Secure Enterprise Client erfolgt dadurch, dass die Lizenzierung und die Software erneuert werden. Dies kann sowohl manuell vorort oder auch über einen Management Server erfolgen.

Beim manuellen Upgrade wird die Software von CD erneut installiert, wobei als zu installierendes Produkt "NCP Secure Enterprise Client" eingegeben wird. Dabei erkennt das Installationsprogramm, dass bereits eine Software-Version installiert ist und führt nach entsprechender Bestätigung ein Update durch (siehe →2.4). Anschließend muss im Popup-Menü der neue Aktivierungsschlüssel mit Seriennummer eingegeben werden.

Bei einem Upgrade über einen Management Server wird im Telefonbuch des Clients die IP-Adresse des Management Servers eingetragen (siehe →Profil-Einstellungen, IP-Adressen-Zuweisung, DNS / WINS). Bei der nächsten Einwahl in das Firmennetz wird die Secure Client Software automatisch herunter geladen. Bei einer erneuten Anwahl mit dieser neuen Software wird eine Profil-Einstellung (CNF-Datei) mit Lizenzierungsschlüssel herunter geladen. Damit ist das Upgrade abgeschlossen.

2.6 Projekt-Logo

Das Logo erscheint in einem Panel des Clients ganz unten über die ganze Breite des Monitors. Für das Logo muss eine Ini-Datei (ProjectLogo.ini) angelegt werden, in der folgendes angegeben werden kann:

- ProjektLogo für kleine Schriftarten
- ProjektLogo für große Schriftarten
- Info-Text (ToolTip) wenn sich der Mauszeiger über dem Logo befindet
- HTML-Datei wenn ein Maus-Click auf das Logo erfolgt.

Bei der Installation wird nachfolgend dargestellte Datei ProjectLogo.ini ins Installations-Verzeichnis kopiert, in der weitere Erläuterungen zum Anlegen des Logos enthalten sind.

```

=====
ProjectLogo.ini
=====
[GENERAL]
Picture_96=
Picture_120=
ToolTip1=
HtmlLocal=

# Picture_96
# =====
# Bitmap des Project-Logos für Ansicht
# mit kleinen Schriftarten (96 DPI)
# Höhe: 24 Pixel (minimal)
# Breite: 328 Pixel (genau)
# Wird kein Pfad angegeben, wird die Datei im aktuellen
# Verzeichnis des Secure Clients gesucht. Z. B.:
#
# Picture_96=C:\Programme\NCP\SecureClient\MyProjectPicture.bmp
#
# Picture_120
# =====
# Bitmap des Project-Logos für Ansicht
# mit großen Schriftarten (120 DPI)
# Höhe: 29 Pixel (minimal)
# Breite: 404 Pixel (genau)
# Wird kein Pfad angegeben, wird die Datei im aktuellen
# Verzeichnis des Secure Clients gesucht. Z. B.:
#
# Picture_96=C:\Programme\NCP\SecureClient\MyProjectPicture.bmp
#
# ToolTip[1] ... ToolTip[X]
# =====
# Info-Text für den ToolTip des Projekt-Logos.
# Pro Zeile im Info-Text muß ein ToolTip-Eintrag mit
# fortlaufender Nummer (ToolTip[x]) erstellt werden.
#
# z.B. ToolTip1=Der Info-Text für des Projekt-Logo
# ToolTip2=-----
# ToolTip3=Dritte Zeile ...
# ToolTip4=Vierte Zeile ...
#
# HtmlLocal
# =====
# HTML-Datei die angezeigt werden soll, wenn ein Maus-Klick auf
# das Projekt-Logo erfolgt. Die Datei muss lokal auf dem Rechner
# verfügbar sein. Wird kein Pfad angegeben, wird die Datei im
# aktuellen Verzeichnis des Secure Clients gesucht. Z. B.:
#
# HtmlLocal=C:\Programme\NCP\SecureClient\MyProjectInfo.html

```

3. Client Monitor

Wenn die Software installiert wurde, kann der Monitor über das Start-Menü → Programme → NCP Secure Client → Secure Entry Client Monitor aktiviert werden. Damit öffnet sich das Fenster des Monitors auf dem Bildschirm.



Hinweis: Wenn der Monitor geladen wurde, erscheint er entweder auf dem Bildschirm oder, wenn er dort nicht dargestellt wird, in der Taskleiste.



Der Monitor hat 4 wichtige Funktionen:

- ☒ den aktuellen Status der Kommunikation wiederzugeben
- ☒ den Verbindungsmodus einzustellen
- ☒ die Limits der Verbindungssteuerung bestimmen
- ☒ die Definition und Konfiguration der Profile zur Anwahl an ein Zielsystem

3.1 Die Oberfläche des Client Monitors

3.1.1 Bedien- und Anzeigefelder

Der Client Monitor besteht aus:

- ☐ einer Titelzeile mit Ampelanzeige,
- ☐ der Hauptmenüleiste,
- ☐ der Profilauswahl mit einem Feld für die Amtsholung,
- ☐ dem grafischen Statusfeld zur Anzeige des Verbindungsstatus,
- ☐ Das Feld mit der Anzeige der Signalstärke wird nur für die Verbindungsarten UMTS /GPRS/WLAN geöffnet
- ☐ der Buttonleiste mit “Verbinden” und “Trennen”
- ☐ und einem Statistikfeld



Die Benutzeroberfläche ist Windows-konform gestaltet und der Bedienung anderer Windows-Anwendungen angepasst. Die Bedienung erfolgt über die Pulldown-Menüs der Menüleiste, über die Buttons der Buttonleiste oder über das Kontextmenü (rechte Maustaste).

3.1.2 Das Erscheinungsbild des Monitors

Je nach gewählter Einstellung im Monitor-Menu “Fenster” erscheint der Monitor nach Ausblenden seiner Bestandteile (siehe weiter unten → Fenster) in verschiedenen Größen.



Das Verbindungsmedium lässt sich im Statistikfeld ablesen oder kann bei der Namensvergabe an das Profil mit eingegeben werden, sodass sie auch im grafischen Statusfeld erscheint.

Modifikationen der Oberfläche



Bitte beachten Sie, dass das Erscheinungsbild des Client Monitors vom Administrator verändert werden kann. Dies betrifft insbesondere die Menüpunkte “Verbindungs-Informationen”, “Zertifikate”, “Verbindungssteuerung” und “Logon Optionen”. Auch Parameterfelder des Telefonbuchs und einzelne Parameter können vom Administrator ausgeblendet bzw. auf “nicht konfigurierbar” gesetzt werden. Die ausgeblendeten und deaktivierten Features und Parameter erleichtern Ihnen den Umgang mit der Software und haben weder Einfluss auf die Leistungsfähigkeit der Software noch auf Ihre Arbeit. Beachten Sie dazu den Abschnitt 4.3 Konfiguration, 4.3.8 Konfigurations-Sperren.

3.1.3 Anwahl über das Profil an das Zielsystem

Sobald die Software installiert mit einem Profil korrekt konfiguriert wurde (siehe unten 4.2.3 Konfiguration), kann die Anwahl an dieses Zielsystem stattfinden.



Das gewünschte Profil wird über die Auswahl-Box unter dem Hauptmenü oder nach Klick auf die rechte Maustaste aus einer Liste gewählt (siehe nebenstehendes Bild).

Um eine Verbindung über das selektierte Profil herzustellen, ist es nicht nötig, den Client Monitor eigens zu starten oder die Anwahl manuell durchzuführen. Lediglich die gewünschte Applikations-Software muss gestartet werden. Die Verbindung wird dann, entsprechend den Parametern des Profils, automatisch aufgebaut (siehe → Verbindungssteuerung, Verbindungsaufbau, automatisch). Daneben ist es auch möglich, manuell die Verbindung herzustellen, indem Sie im Monitor den Hauptmenüpunkt "Verbindung" anklicken und "Verbinden" wählen. Alternativ kann auch der Button "Verbinden" angeklickt werden (siehe → Verbindungsaufbau).



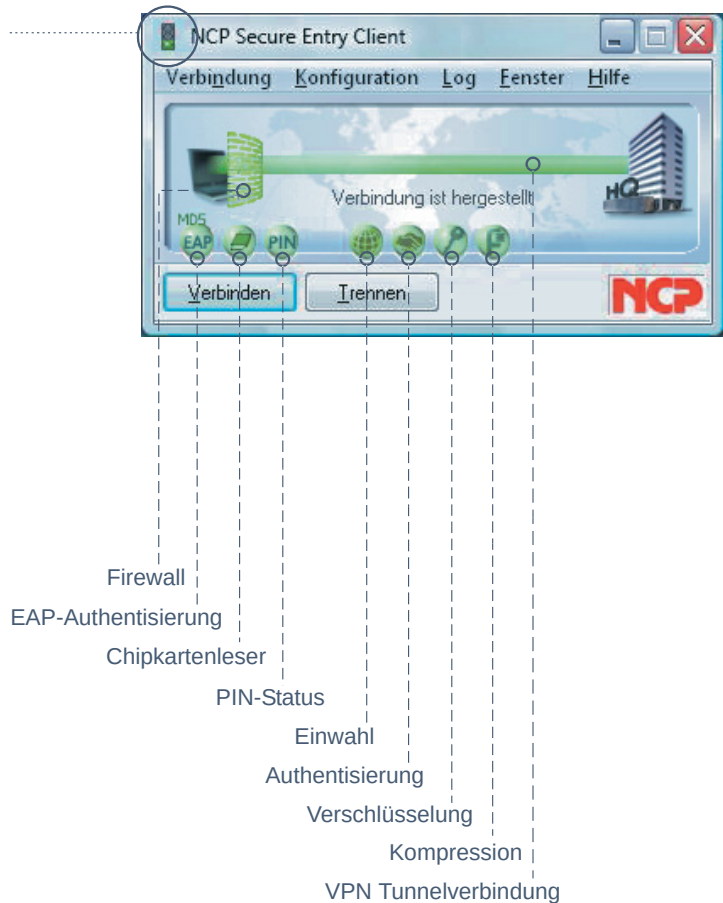
Eine bestehende Verbindung (siehe → Bild oben) wird mit einem dicken grünen, durchgehenden Balken zwischen Client und Server dargestellt, unter dem der Text "Verbindung ist hergestellt" eingeblendet wird. Gleichzeitig wird die (Icon-)Ampel grün. Damit werden Sie darauf aufmerksam gemacht, dass für eine Remote-Verbindung Gebühren anfallen.

3.1.4 Die Symbole des Monitors

Die Monitoroberfläche des Clients ist informativ mit Symbolen gestaltet. Je nach Anzeige und Farbe geben sie Auskunft über den aktuellen Status der Verbindung oder einzelne konfigurierte Features.

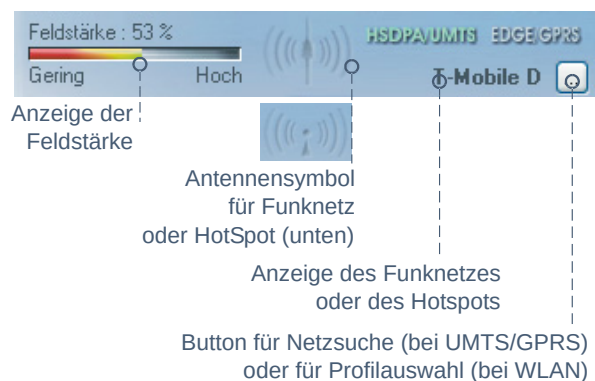
Das Ampelsymbol ist immer sichtbar wenn der Client gestartet ist. Ist der Monitor minimiert, d. h. geschlossen, erscheint es in der Task-Leiste. Mit einem Doppelklick auf dieses Icon kann der Monitor wieder geöffnet werden. Erst wenn der Monitor beendet wird, verschwindet auch das Ampelsymbol.

Die weiteren Symbole sind auf den folgenden Seiten ausführlich erklärt.



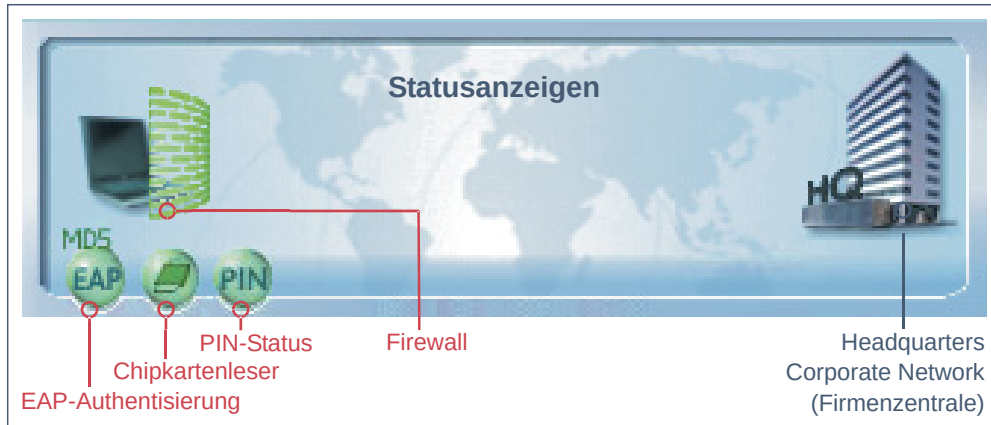
Je nach Konfiguration und Installation einer Multifunktionskarte erscheint zusätzlich alternativ ein WLAN- oder UMTS / GPRS-Panel im Monitor.

Im UMTS / GPRS-Panel kann das gewünschte Datenübertragungsverfahren durch Klick auf den jeweiligen Schriftzug gewählt werden. Es wird dann grün dargestellt.



3.1.5 Statusanzeigen

Das grafische Feld des Client-Monitors zeigt je nach Konfiguration verschiedene Icons, sie während der Phasen des Verbindungsaufbaus einen jeweils verschiedenen Status annehmen können. Hinweise zu ihrer Bedeutung geben Kurzinfos, sobald der Mauszeiger über eines der Icons streift. Im folgenden sind die Statusanzeigen, wie in untenstehender Abbildung, von links nach rechts beschrieben.



■ EAP-Authentisierung



Wenn eine erweiterte Authentisierung mittels Extensible Authentication Protocol (EAP) in den "EAP-Optionen" aktiviert wurde, wird dies mit dem EAP-Icon angezeigt. Die Farbe **Gelb** symbolisiert die EAP-Verhandlungsphase, **Rot** eine fehlgeschlagene Authentisierung, die Farbe **Grün** die erfolgreiche Authentisierung mit EAP. Durch einen Doppelklick auf das EAP-Symbol kann das EAP zurückgesetzt werden. Anschließend erfolgt automatisch eine erneute EAP-Verhandlung.



Bei erfolgreicher Authentisierung gegenüber einer Netzwerkkomponente, gibt die Gegenstelle zurück, welches Protokoll verwendet wurde, was immer mit einem Symbol in **Grün** und der Bezeichnung MD5 oder TLS dargestellt wird.



Erscheint EAP-Symbol in der Farbe **Rot** und die Verbindung wurde trotzdem aufgebaut, so bedeutet dies, dass im Client EAP konfiguriert wurde, die Netzwerkkomponente jedoch kein EAP benötigt.

■ Chipkartenleser



Wurde ein Chipkartenleser installiert und konfiguriert (siehe im Monitormenü → Konfiguration / Zertifikat), so wird sein Symbol in **Blau** dargestellt.



Wird die Chipkarte in den Leser gesteckt, wechselt die wird das Symbol in **Grün** dargestellt.

■ PIN-Status



Ein PIN-Symbol in der Farbe **Grau** symbolisiert immer, dass die PIN für das jeweils konfigurierte Zertifikat noch eingegeben werden muss. Ein Doppelklick auf dieses Symbol öffnet den Dialog zur Eingabe der PIN. Ein falsche PIN wird mit einer Fehlermeldung quittiert, wobei gleichzeitig die noch möglichen PIN-Eingaben heruntergezählt werden.



Nach korrekter PIN-Eingabe wird das Symbol in **Grün** dargestellt. Diese Farbe zeigt an, dass die eingegebene PIN gültig ist, auch wenn keine Verbindung aufgebaut ist! Wollen Sie sicherstellen, dass kein Unbefugter bei Ihrer Abwesenheit eine Verbindung herstellen kann, so muss die PIN zurückgesetzt werden (siehe Monitormenü → Verbindung / PIN zurücksetzen) oder unter “Konfiguration / Zertifikat” die Funktion “PIN-Abfrage bei jedem Verbindungsaufbau” aktiviert sein. In letzterem Fall erscheint der Dialog zur PIN-Eingabe nicht nach Doppelklick auf das graue Symbol, sondern erst nachdem Verbindungsaufbau.

■ Firewall



Das Firewall-Symbol ist immer dann sichtbar, wenn eine Firewall aktiviert ist. Ist die globale Firewall (Personal Firewall) mit definierten Regeln aktiv und die link-spezifische Firewall nicht aktiv, so wird das Symbol ohne Pfeile in der Farbe **Rot** dargestellt.



Wurde vom Administrator ein Friendly Net (Friendly Net Detection) festgelegt, und befindet sich der Client darin, so wird das Firewall-Symbol in der Farbe **Grün** dargestellt. Die Friendly Net Detection wird im Monitor-Konfigurationsmenü unter “Firewall-Einstellungen / Bekannte Netze” vorgenommen, entweder indem statische Netzwerk-Routen angegeben werden, oder indem die automatische Erkennung der bekannten Netze aktiviert wird. Siehe dazu die Beschreibung unter “Firewall-Einstellungen / Konfigurationsfeld - Bekannte Netze”.

Bei aktivierter Link Firewall wird das Symbol mit Pfeilen dargestellt, gleich ob die globale Firewall aktiv oder inaktiv ist.



Wird die Link Firewall im Telefonbuch aktiv geschaltet mit “Stateful Inspection aktivieren → immer” und wird konfiguriert, dass eine Kommunikation ausschließlich im Tunnel zugelassen wird, so wird das Firewall-Symbol mit **zwei roten Pfeilen** dargestellt.



Wird die Option “Ausschließlich Kommunikation im Tunnel zulassen” ausgeschaltet, so wird das Symbol mit einem **grünen und einem roten Pfeil** dargestellt.

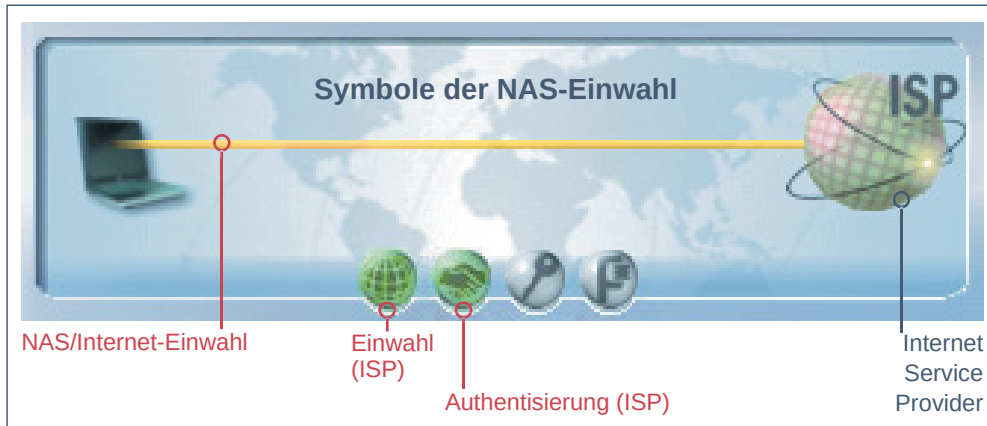
Wird Stateful Inspection nur bei einer bestehenden Verbindung aktiviert, so erscheinen die Pfeil-Symbole nur nach einem Verbindungsaufbau.



Die **Pfeil-Symbole** erscheinen **vor einer grünen Firewall**, wenn zusätzlich zu Optionen der Link Firewall ein Friendly Net in der globalen Firewall definiert wurde, worin sich sich der Client aktuell befindet.

3.1.6 Symbole des Verbindungsaufbaus

Neben den Statusanzeigen enthält das grafische Feld des Client-Monitors auch Symbole des Verbindungsaufbaus.



■ Symbole der NAS-Einwahl

Findet eine Einwahl zu einem Network Access Server bzw. Internet-Dienste-Anbieter (ISP) ins Internet statt, so wird die Einwahlverbindung mit einer dünnen gelben Linie symbolisiert. Die Einwahl ist abgeschlossen und die Verbindung zum ISP erfolgreich hergestellt, wenn die dünne Verbindungslinie die Farbe Grün annimmt.

Gleichzeitig mit dem Start des Verbindungsaufbaus ändern sich auch die Farben der Symbole für die NAS-Einwahl.

Die Einwahl am ISP ist mit einem Globus dargestellt, die Authentisierung am ISP mit einem Händeschütteln. Ihre Farben wechseln während des Verbindungsaufbaus von grau zu blau, blinken dann grün, um schließlich bei erfolgreichem Verbindungsaufbau grün stehen zu bleiben.

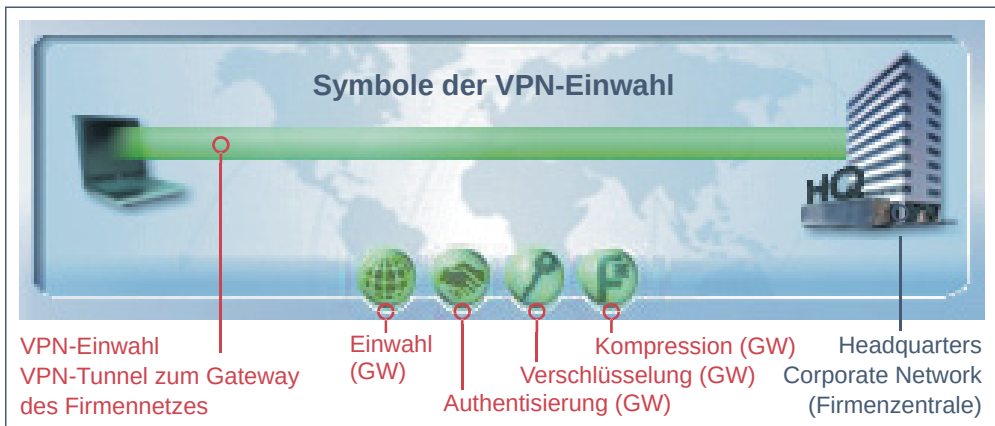


Die Parameter für die NAS-Einwahl befinden sich in den Profil-Einstellungen unter "Netzeinwahl". Soll das Profil für die "automatische Medienerkennung" (siehe → Profil-Einstellungen / Grundeinstellungen) verwendet werden, so muss unter "Netzeinwahl" unbedingt ein Benutzername und ein Passwort eingegeben sein.

■ Symbole der VPN-Einwahl

Nach abgeschlossener NAS-Einwahl kann die VPN-Einwahl zum Firmen-Gateway stattfinden. Dabei wird die Einwahlverbindung mit einer dicken gelben Linie symbolisiert. Die Einwahl ist abgeschlossen und die Verbindung zum VPN Gateway erfolgreich hergestellt, wenn die dicke Verbindungslinie die Farbe Grün annimmt.

Gleichzeitig mit dem Start des Verbindungsaufbaus zum Gateway ändern sich auch die Farben der Symbole für die VPN-Einwahl. Die Einwahl und die Authentisierung am VPN Gateway ist genauso wie bei der NAS-Einwahl dargestellt. Hinzu kommen noch die Symbole für die Schlüsselverhandlung (Schlüssel) und die Kompression (Zange), sofern deren Konfiguration von Seiten des Gateways vorgeschrieben ist.



Die Farben der Symbole der VPN-Einwahl wechseln von grau zu blau, blinken dann grün, um schließlich bei erfolgreichem Verbindungsaufbau grün stehen zu bleiben. Dabei muss der Vorgang der Einwahl und Authentisierung am VPN Gateway immer durchlaufen werden, Verschlüsselung und Kompression sind optional. Die Symbole der VPN-Einwahl sind von links nach rechts:



Einwahl am VPN Gateway:

Die Zieladresse des VPN-Gateways wird in den Profil-Einstellungen unter "IPSec-Einstellungen / Gateway" angegeben.



Authentisierung am VPN Gateway:

Die nötigen Parameter befinden sich in den Profil-Einstellungen unter "Identität". Verwendet wird immer "Extended Authentication (XAUTH)". Benutzername und Passwort werden entweder aus der Konfiguration unter diesem Parameter oder aus einem Zertifikat ausgelesen. Ein zu verwendendes Zertifikat wird im Monitor-Menü unter "Konfiguration / Zertifikate" konfiguriert, wobei das Aussteller-Zertifikat des anzuwählenden Gateways mit dem Benutzer-Zertifikat zusammenpassen muss.



Verschlüsselung:

Zur Verschlüsselung dient entweder ein Pre-shared Key oder der Private Key aus einem Zertifikat. Beide Alternativen werden in den Profil-Einstellungen unter "Identität" eingestellt. Wird der "Pre-shared Key" verwendet, muss das "Shared Secret" hier eingetragen werden. Wird der "Pre-shared Key" nicht verwendet, wird automatisch das Zertifikat benutzt. Welche Verschlüsselung benutzt werden muss gibt das Gateway vor.



Kompression:

Kompression wird nur genutzt, wenn sie auch vom Gateway unterstützt wird. Eingestellt wird sie in den Profil-Einstellungen unter "Erweiterte IPSec-Optionen / IP-Kompression verwenden".

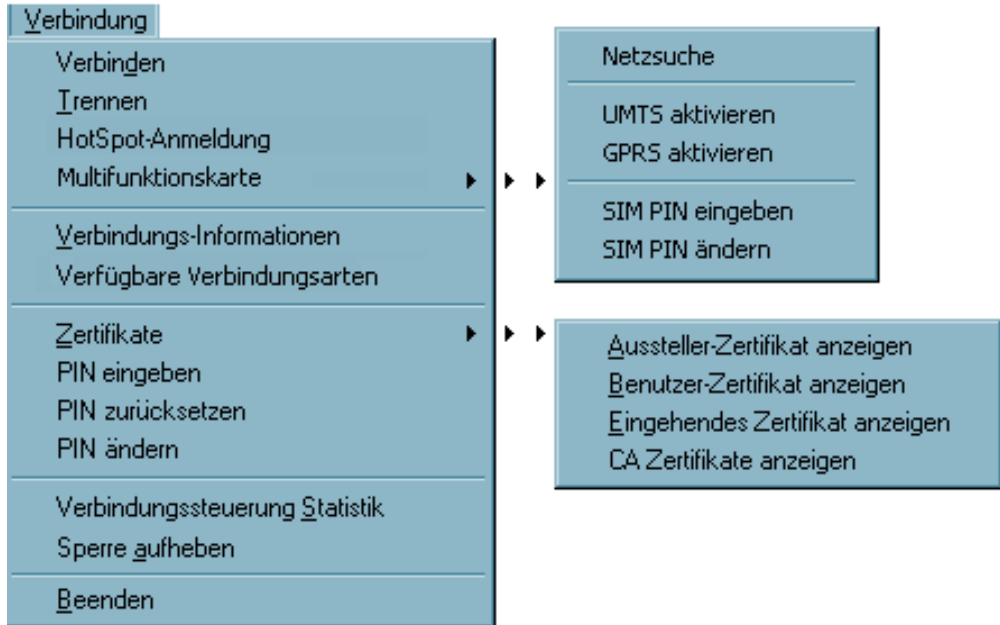
4. Monitor-Bedienung

Diese Beschreibung folgt den Menüpunkten in der Menüleiste.

Die Hauptmenüpunkte in der Menüleiste von links nach rechts sind:

- ☐ Verbindung
- ☐ Konfiguration
- ☐ Log
- ☐ Fenster
- ☐ Hilfe

4.1 Verbindung



Unter diesem Menüpunkt befinden sich die Kommandos zum Aufbau und Trennen einer Verbindung, Informationsfenster zum aktuellen Verbindungsaufbau sowie zur Darstellung der eingesetzten Zertifikate. Die PIN für das Zertifikat kann hier eingegeben und ggf. geändert werden. Außerdem kann hier die Statistik der Verbindungssteuerung abgelesen werden und gegebenenfalls die Sperre der Verbindungssteuerung gelöst werden, wenn ein von Ihnen gesetztes Limit überschritten wurde.

4.1.1 Verbinden

Mit diesem Befehl wird eine Verbindung aufgebaut. Eine Verbindung kann nur aufgebaut werden, wenn ein “Ziel” aus dem “Telefonbuch” selektiert ist (siehe → Telefonbuch, Zielsystem).

Wenn Sie die Funktion “Verbinden” wählen, wird die Anwahl an das ausgewählte Zielsystem manuell durchgeführt. Der jeweilige Status des Verbindungsaufbaus wird grafisch dargestellt (siehe → Eine Verbindung herstellen). Wenn Sie, je nach Zielsystem, die Verbindung manuell oder automatisch herstellen wollen, so können Sie dies im Telefonbuch mit dem Parameter “Verbindungsaufbau” im Feld “Verbindungssteuerung” definieren (siehe → Telefonbuch, Verbindung).

4.1.2 Trennen

Mit diesem Befehl wird eine Verbindung abgebaut. Mit der Funktion “Trennen” wird der Abbau der aktuell bestehenden Verbindung manuell durchgeführt. Wenn die Verbindung abgebaut wurde, wechselt die Ampellampe für die gesamte Offline-Dauer von grün auf rot.

4.1.3 HotSpot-Anmeldung



Voraussetzungen: Der Rechner muss sich mit aktivierter WLAN-Karte im Empfangsbereich eines HotSpots befinden. Die Verbindung zum HotSpot muss hergestellt und eine IP-Adresse für den Wireless-Adapter muss zugewiesen sein. (Unter Windows XP steht eine entsprechende Konfiguration für den Zugriff auf WLANs zur Verfügung.)

Die Firewall des NCP Secure Clients sorgt dafür, dass lediglich die IP-Adresszuweisung per DHCP erfolgen darf, weitere Zugriffe ins WLAN bzw. vom WLAN werden unterbunden. Die Firewall gibt dynamisch die Ports für http bzw. https für die Anmeldung bzw. Abmeldung am HotSpot frei. Dabei ist nur Datenverkehr mit dem HotSpot Server des Betreibers möglich. Ein öffentliches WLAN wird auf diese Weise ausschließlich für die VPN-Verbindung zum zentralen Datennetz genutzt. Direkter Internet-Zugriff ist ausgeschlossen. Damit die Anmeldeseite des HotSpots im Browser geöffnet werden kann, muss eine eventuelle Proxy-Konfiguration deaktiviert werden.

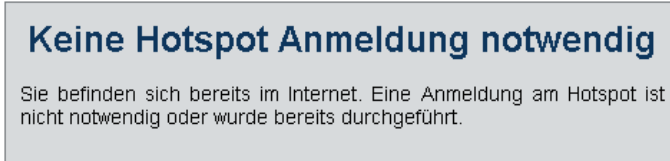


Derzeit unterstützt die HotSpot-Anmeldung des Clients ausschließlich HotSpots, die mit einer Umleitung (Redirect) einer Anfrage mit einem Browser auf die Anmeldeseite des öffentlichen WLAN-Betreibers arbeiten (z. B. T-Mobile oder Eurospot).

Sind obige Voraussetzungen erfüllt, so öffnet ein Klick auf den Menüpunkt “HotSpot-Anmeldung” die Website zur Anmeldung im Standard-Browser. Nach Eingabe der Zugangsdaten kann die VPN-Verbindung z. B. zur Firmenzentrale aufgebaut und sicher kommuniziert werden.

Die HotSpot-Anmeldung erfolgt über das Monitor-Menü “Verbindung / HotSpot-Anmeldung”. Nachdem dieser Menüpunkt angeklickt wurde, können verschiedene Verbindungsmeldungen am Bildschirm erscheinen:

– Wenn sich der Benutzer bereits im Internet befindet, wird er mit der Startseite <http://www.ncp.de> verbunden. Es erscheint ein Fenster mit folgender Meldung:



Dieser Text kann vom Administrator ausgetauscht werden, indem die Adresse einer anderen HTML-Startseite in der Form angegeben wird

<http://www.mycompagnie.de/error.html>
und der Text von error.html entsprechend geändert wird.

– Ist der Benutzer noch nicht angemeldet, erscheint ein Fenster mit der Aufforderung Benutzernamen und Passwort für die Anmeldung am HotSpot-Betreiber einzugeben.

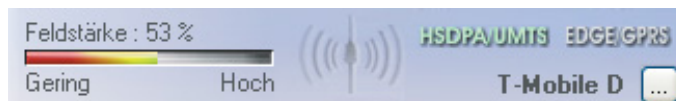
– Wenn der Benutzer keine Website erreicht, erscheint die Microsoft-Fehlermeldung “... not found”.

4.1.4 Multifunktionskarte

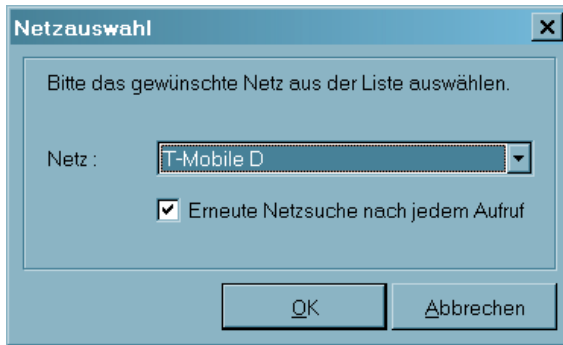
Nachdem eine Multifunktionskarte installiert wurde (siehe dazu auch den Anhang dieses Handbuchs), wird dieser Menüpunkt dargestellt. Außerdem wird das Feld mit der Anzeige für UMTS / GPRS im Monitor eingeblendet und das WLAN-Panel ausgeblendet (siehe oben “Symbole des Monitors”).

■ Netzsuche

Die installierte Multifunktionskarte sucht nach dem Start des Monitors automatisch nach einem Funknetz und zeigt es mit der entsprechenden Feldstärke an, sobald es gefunden wurde (T-Online im Bild unten). Durch Anwahl des Menüpunkts oder des Buttons für “Netzsuche” kann eine erneute Netzsuche ausgelöst werden.



Bei zu geringer Feldstärke schaltet die Karte automatisch von der Datenübertragungstechnik UMTS auf GPRS, wobei die Verbindung bestehen bleibt. Erhöht sich die Feldstärke wieder, schaltet die Karte automatisch wieder zurück.

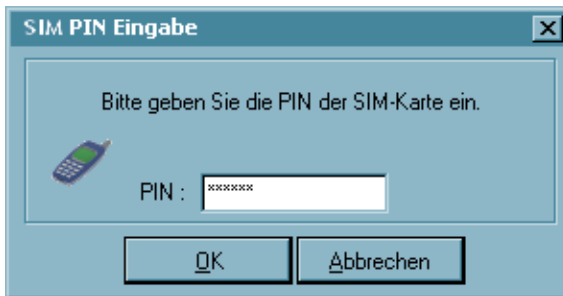


Wurde eine Netzsuche durchgeführt, wird das Fenster zur Netzauswahl eingeblendet (links). Das gewünschte Netz kann aus einer Liste ausgewählt werden. Wird die erneute Netzsuche nach jedem Aufruf des Monitors nicht gewünscht, so muss die standardmäßig aktive Funktion über den Check-Button ausgeschaltet werden.

■ GPRS / UMTS aktivieren

Die Datenübertragungstechnik kann auch manuell gewechselt werden. Dazu wird mit der Maus der Text mit der gewünschten Übertragungstechnik angeklickt oder dieser Menüpunkt gewählt. Bei einem manuellen Wechsel des Mediums wird die Verbindung zunächst abgebaut. Die Verbindung wird dann wieder automatisch aufgebaut, wenn "automatischer Verbindungsaufbau" im Telefonbuch konfiguriert wurde.

■ SIM PIN eingeben



Der Dialog zur Eingabe der SIM PIN erscheint automatisch bei einem Verbindungsaufbau.

Über diesen Menüpunkt kann die SIM PIN auch vor einem Verbindungsaufbau eingegeben werden.

■ SIM PIN ändern

Die Änderung der SIM PIN kann nur vorgenommen werden, wenn die bisherige SIM PIN korrekt eingegeben wurde.

■ PUK Eingabe

Nach dreimaliger Falscheingabe der SIM PIN erscheint das Fenster zur Eingabe des PUK (Personal Unblocking Key), welcher der SIM-Karte beiliegt. Nach korrekter Eingabe des PUK kann eine neue SIM PIN eingegeben werden.

4.1.5 Verbindungs-Informationen

Wenn Sie den Menüpunkt “Verbindungs-Informationen” anklicken, werden statistische Werte gezeigt. Darüber hinaus aber auch welche Security-Schlüssel (SSL mit Zertifikat, Blowfish ...) verwendet werden und welche IP-Adressen über PPP-Verhandlung zwischen Client und Server ausgetauscht werden.

Protokoll	Tx (Byte)	Rx (Byte)
IP :	0	0
Gesamt :	0	0

Statistik	
Profil :	Zentrale (ISDN)
Verbindungszeit :	00:00:00
Timeout (sec):	0
Richtung :	out
Durchsatz (KByte/s):	0,000
Verbindungsmedium :	ISDN
Multi-Link :	Aus
Kompression :	Aus

Die Verbindungs-Informationen können vom Administrator ausgeblendet werden, so dass der Menüpunkt nicht aktiviert werden kann.



Sind die Verbindungs-Informationen ausgeblendet, so können die wichtigsten Daten aus den Feldern der Datenübertragung, der Statistik und der Sicherheit auch aus dem Statistik-Fenster des Clients abgelesen werden (siehe → 3.2.5 Fenster, Statistik anzeigen).

■ Verbindungszeit

Als Verbindungszeit wird die gesamte Zeitdauer der Verbindung zu einem bestimmten Gateway angezeigt, unabhängig von irgendwelchen Timeouts. Der Wert für die Verbindungszeit wird nur dann auf null (0) gesetzt, wenn die Verbindung zu einem anderen Gateway hergestellt oder der PC gebootet wird.

■ Timeout

Der Monitor zeigt die Zeit an, die bis zum nächsten Timeout noch verbleibt. Unmittelbar nachdem der letzte Datenaustausch erfolgt ist (einschließlich Handshake) beginnt die Uhr für den Timeout zu laufen. (Siehe → Telefonbuch, Line Management).

■ Richtung

Unter dieser Rubrik wird die Richtung der Kommunikation wie folgt angezeigt:

Out = ein ausgehender Ruf wird auf diesem Kanal registriert

In = ein ankommender Ruf wird auf diesem Kanal registriert.

■ Durchsatz

Die angezeigte Zahl schwankt entsprechend dem aktuellen Datendurchsatz.

■ Multilink

Besteht die Verbindung über mehrere ISDN-B-Kanäle, so wird hier "on" angezeigt.

■ Verbindungsmedium

Folgende Verbindungsmedium werden unterstützt: ISDN-, Modem, LAN over IP, xDSL (PPPoE), xDSL (AVM - PPP over CAPI), GPRS, WLAN und PPTP.

■ Kompression

Kompression wird immer vom Gateway definiert. IPSec-Kompression wird mit "IPSec Compression (LZS)" angezeigt.

■ Verschlüsselung

Der verwendete Verschlüsselungsalgorithmus wird angezeigt. Folgende Typen werden unterstützt: AES, Blowfish, 3DES. Die Verschlüsselungsart wird vom Zentralsystem vorgegeben.

■ Schlüsselaustausch

Hier wird angezeigt, auf welche Art der Austausch des Session Keys erfolgt:

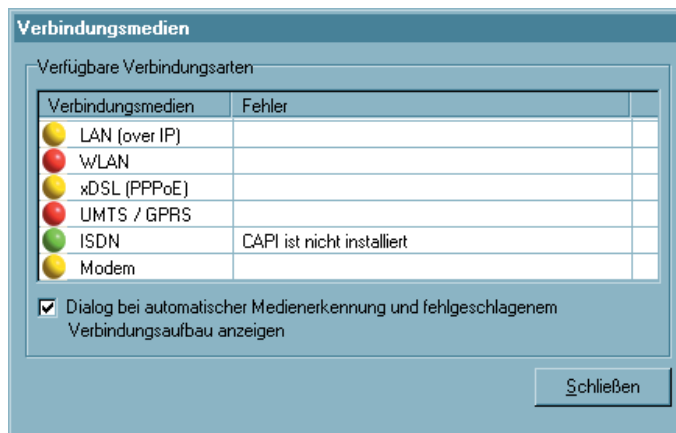
Static Key Der Schlüssel muss am Client und am Zentralsystem übereinstimmen. Er wird in der Profil-Einstellung unter "Identität" eingetragen

IKE (IPSec) Zur Übertragung des Session Keys wird der verschlüsselte Kontrollkanal der Phase-1-Verhandlung verwendet.

■ Rx und Tx Bytes

Rx und Tx Bytes zeigt die Datenmenge an, die gesendet (out) und empfangen (in) wird. Die Gesamtmenge (Total) und die nach Protokoll unterschiedenen Datenmengen werden in Bytes angezeigt (1 Byte = 1 Zeichen).

4.1.6 Verfügbare Verbindungsarten



Dieses Fenster dient ausschließlich der Benutzerinformation über die zur Verfügung stehenden Verbindungsarten und das aktuell genutzte Medium. Sind wechselweise unterschiedliche Verbindungsarten genutzt, so erkennt der Client automatisch, welche Medien aktuell zur Verfügung stehen und wählt davon das schnellste aus.

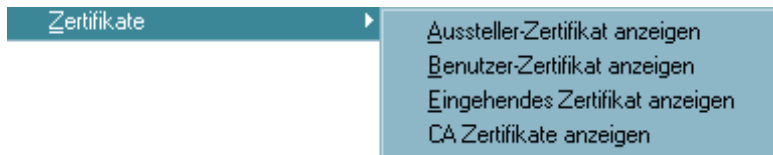
Die zur Verfügung stehenden Verbindungsarten werden mit gelber Signallampe dargestellt, die ausgewählte Verbindungsart mit einer grünen.

Mit der Checkbox kann eingestellt werden, dass dieses Fenster bei automatischer Medieneerkennung selbständig aufgeblendet wird, wenn der Verbindungsaufbau fehlgeschlagen ist. Das Fenster wird auch dann am Bildschirm eingeblendet, wenn der Client-Monitor minimiert ist. Hinter der genutzten Medienart wird der Fehler bezeichnet.



Zur Konfiguration der automatischen Medieneerkennung beachten Sie in den Profil-Einstellungen das Parameterfeld "Grundeinstellungen".

4.1.7 Zertifikate



Im Pulldown-Menü “Verbindung” finden Sie den Menüpunkt “Zertifikate” mit den Menüabzweigungen “Konfiguration”, “Aussteller-Zertifikat anzeigen”, “Eingehendes Zertifikat anzeigen” und “CA-Zertifikate anzeigen”.

Zertificate (Certificates) werden von einer CA (Certification Authority) mittels PKI-Manager (Software) ausgestellt und auf eine Smart Card (Chipkarte) gebrannt. Diese Smart Card enthält u.a. mit den Zertifikaten digitale Signaturen, die ihr den Status eines digitalen Personalausweises verleihen.

■ Aussteller-Zertifikat anzeigen

Wenn Sie sich das Aussteller-Zertifikat anzeigen lassen, können Sie sehen welche Merkmale zur Erstellung des Zertifikats genutzt wurden, z.B. die eindeutige E-Mail-Adresse.

Aussteller (CA)	=	Benutzer und Aussteller eines Aussteller-Zertifikates sind für gewöhnlich identisch (selfsigned certificate). Der Aussteller des Aussteller-Zertifikats muss mit dem Aussteller des Benutzer-Zertifikats identisch sein (siehe → Benutzer-Zertifikat anzeigen).
Seriennummer	=	Nach der Seriennummer werden die Zertifikate mit den in der Revocation List der Certification Authority gehaltenen verglichen.
Gültigkeitsdauer	=	Die Gültigkeitsdauer der Zertifikate ist beschränkt. Die Gültigkeitsdauer eines Aussteller(Root)-Zertifikats ist in aller Regel länger als die eines Benutzer-Zertifikats. Mit dem Erlöschen der Gültigkeit des Aussteller-Zertifikats erlischt automatisch die Gültigkeit eines vom gleichen Aussteller ausgestellten Benutzer-Zertifikates.
Fingerprint	=	Hash-Wert. Der mit dem Private Key der CA verschlüsselte Hash-Wert ist die Signatur des Zertifikats.

■ Benutzer-Zertifikat anzeigen

Wenn Sie sich Ihr Benutzer-Zertifikat anzeigen lassen, können Sie sehen welche Merkmale zur Erstellung des Zertifikats genutzt wurden, z.B. die eindeutige E-Mail-Adresse.

Austeller (CA)	=	Der Aussteller Ihres Benutzer-Zertifikates muss mit dem Aussteller des Aussteller-Zertifikates identisch sein. (siehe → Aussteller-Zertifikat anzeigen).
Seriennummer	=	Nach der Seriennummer werden die Zertifikate mit den in der Revokation List der Certification Authority gehaltenen verglichen.
Gültigkeitsdauer	=	Die Gültigkeitsdauer der Zertifikate ist beschränkt. Die Gültigkeitsdauer eines Aussteller(Root)-Zertifikats ist in aller Regel länger als die eines Benutzer-Zertifikats. Mit Erlöschen der Gültigkeit geht auch die Funktion des Zertifikats verloren.
Fingerprint	=	Hash-Wert. Der mit dem Private Key der CA verschlüsselte Hash-Wert ist die Signatur des Zertifikats.

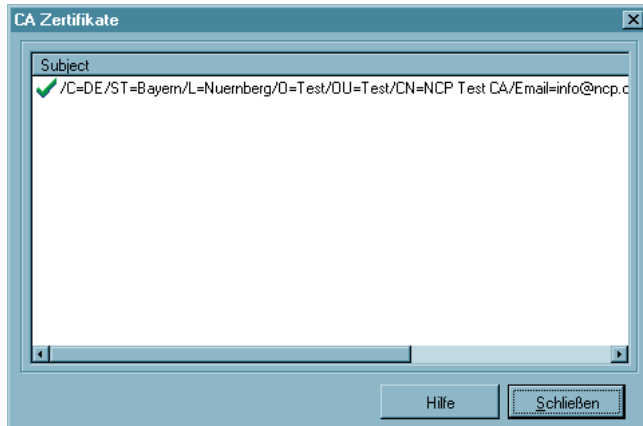
■ Eingehendes Zertifikat anzeigen

Anzeige des Zertifikats, das bei der SSL-Verhandlung von der Gegenstelle (VPN Gateway) übermittelt wird. Sie können z.B. sehen, ob Sie den hier gezeigten Aussteller in der Liste Ihrer CA-Zertifikate (siehe unten) aufgenommen haben.

Ist das eingehende Benutzer-Zertifikat einer der CAs aus der Liste “CA-Zertifikate anzeigen” nicht bekannt, kommt die Verbindung nicht zustande.

Sind keine CA-Zertifikate im Installations-Verzeichnis unter CACERTS\ gespeichert, so findet keine Überprüfung statt.

■ CA-Zertifikate anzeigen



Mit der Client Software werden mehrere Aussteller-Zertifikate unterstützt (Multi CA-Unterstützung). Dazu müssen die Aussteller-Zertifikate im Installations-Verzeichnis unter CACERTS\ gesammelt werden. Im Monitor des Clients wird die Liste der eingespielten CA-Zertifikate angezeigt unter dem Menüpunkt "Verbindung → Zertifikate → CA-Zertifikate".

Wird das Aussteller-Zertifikat einer Gegenstelle empfangen, so ermittelt der Client den Aussteller und sucht anschließend das Aussteller-Zertifikat, zunächst auf Smart Card oder PKCS#12-Datei, anschließend im Installations-Verzeichnis unter CACERTS\.

Ist das Aussteller-Zertifikat nicht bekannt, kommt die Verbindung nicht zustande (No Root Certificate found). Sind keine CA-Zertifikate im Installations-Verzeichnis unter CACERTS\ vorhanden, so wird keine Verbindung unter Einsatz von Zertifikaten zugelassen.

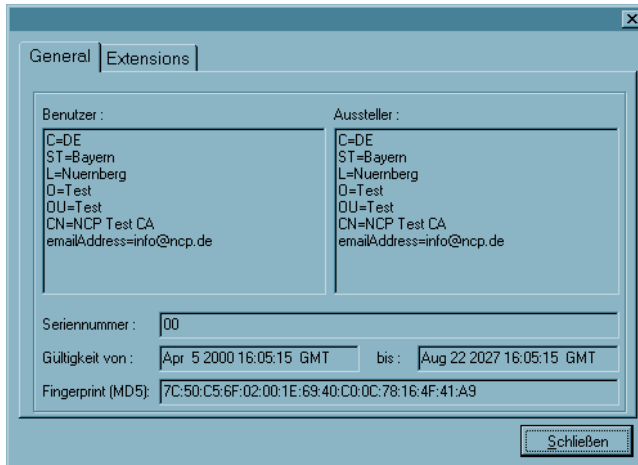
■ Anzeige und Auswertung von Erweiterungen bei eingehenden Zertifikaten und CA-Zertifikaten

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zertifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

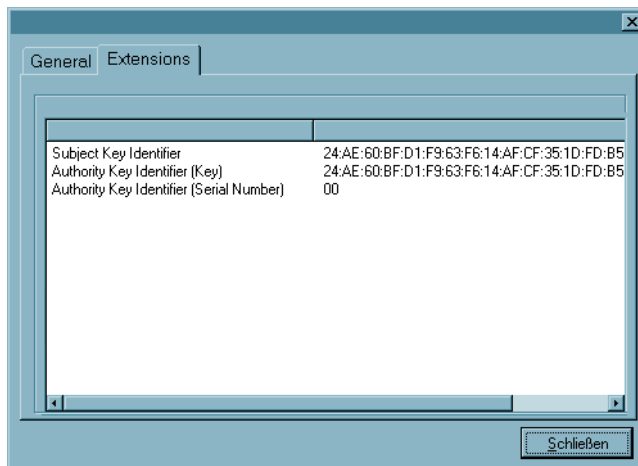
Für den IPSec Client und das Gateway sind drei Erweiterungen von Bedeutung:

- ☐ extendedKeyUsage
- ☐ subjectKeyIdentifier
- ☐ authorityKeyIdentifier

Anzeige der Erweiterungen (Extensions)



Um sich die Erweiterungen eines eingehenden oder CA-Zertifikats anzeigen zu lassen, kann wie folgt vorgegangen werden: Das CA-Zertifikat, dessen Erweiterungen angezeigt werden sollen, muss mit einem Doppelklick im Fenster für CA-Zertifikate (siehe oben) geöffnet werden. Damit wird nebenstehendes Anzeigefeld mit den allgemeinen Daten (General) geöffnet.



Für das jeweils eingehende Zertifikat wird dieses Feld bereits geöffnet, nachdem "Eingehendes Zertifikat anzeigen" im Zertifikats-Menü gewählt wurde. Das Ansichtsfeld "General" zeigt die allgemeinen Zertifikatsdaten (siehe Bild oben).

Das Ansichtsfeld "Extensions" zeigt die Zertifikatserweiterungen, sofern sie vorhanden sind (siehe Bild links).

Auswertung der Erweiterungen (Extensions)

KeyUsage

Ist in einen eingehenden Zertifikat die Erweiterung KeyUsage enthalten, so wird diese überprüft. Folgende KeyUsage-Bits werden akzeptiert:

- Digital Signatur
- Key Encipherment (Schlüsseltransport, Schlüsselverwaltung)
- Key Aggrement (Schlüsselaustaschverfahren)

Ist eines des Bits nicht gesetzt, wird die Verbindung abgebaut.

extendedKeyUsage

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der Secure Client, ob der definierte erweiterte Verwendungszweck die “SSL-Server-Authentisierung” ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck “SSL-Server-Authentisierung” beinhalten muss. Dies gilt auch bei einem Rückruf an den Client über VPN.

Ausnahme: Bei einem Rückruf des Servers an den Client nach einer Direkteinwahl ohne VPN aber mit PKI prüft der Server das Zertifikat des Clients auf die Erweiterung extendedKeyUsage. Ist diese vorhanden, muss der Verwendungszweck “SSL-Server-Authentisierung” beinhaltet sein, sonst wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

subjectKeyIdentifier / authorityKeyIdentifier

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann kein CA-Zertifikat gefunden werden, wird die Verbindung abgelehnt.

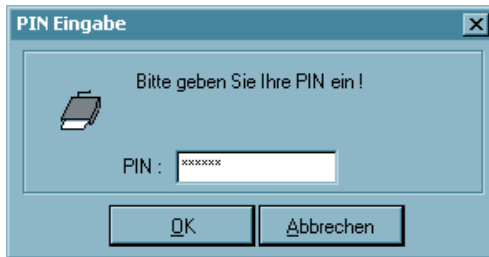
CDP (Certificate Distribution Point)

Im Certificate Distribution Point ist die URL für den Download einer CRL hinterlegt. Ist im Zertifikat die Erweiterung CDP enthalten, wird nach dem Verbindungsaufbau die CRL über die angegebene URL heruntergeladen und überprüft. Wird dabei festgestellt, dass das Zertifikat ungültig ist, wird die Verbindung abgebaut. Die CRL wird dabei unter dem Common-Name der CA im Verzeichniss ncple\crls gespeichert.

4.1.8 PIN eingeben

Die PIN-Eingabe kann bereits vor einem Verbindungsaufbau erfolgen, nachdem der Monitor gestartet wurde. Wird zu einem späteren Zeitpunkt eine Verbindung aufgebaut, die ein Zertifikat erfordert, so kann dann die PIN-Eingabe unterbleiben – es sei denn, die Konfiguration zum Zertifikat verlangt dies (siehe → Konfiguration, Zertifikate).

Wenn Sie den IPSec Client zur Verwendung einer Smart Card konfiguriert haben (siehe → Konfiguration / Zertifikate), erscheint ein hellblaues Symbol für die Smart Card. Wenn Sie Ihre Smart Card in den Reader gesteckt haben, ändert sich die Farbe von hellblau zu grün.



Sobald Sie die erste Verbindung aufbauen wollen, für die ein Zertifikat genutzt wird, wird ein Dialog zur PIN-Eingabe geöffnet – sofern Sie die PIN noch nicht vorher eingegeben haben. Bei einem wiederholten manuellen Verbindungsaufbau kann die PIN-Eingabe unterbleiben, wenn nicht anders konfiguriert (siehe → Konfiguration, Zertifikat).



Wird ein Soft-Zertifikat verwendet, so kann die PIN 4-stellig sein. Wird eine Chipkarte verwendet, muss die PIN mindestens 6-stellig sein.



Fehlerhafte Eingaben und falsche PINs werden nach ca. 3 Sekunden mit einer Fehlermeldung quittiert. Ein Verbindungsaufbau ist dann nicht möglich. Nach dreimaliger fehlerhafter Eingabe der PIN, wird die PIN gesperrt! Wenden Sie sich in diesem Fall an Ihren Remote-Administrator. Wenn die Chipkarte während des laufenden Betriebs entfernt wird, findet ein Verbindungsabbau statt.

Erst nach korrekter PIN-Eingabe erfolgt der Verbindungsaufbau.

Sicherung der PIN-Benutzung

Ist in der Zertifikatskonfiguration die Funktion "PIN-Abfrage bei jedem Verbindungsaufbau" aktiviert, wird der Menüpunkt "PIN eingeben" automatisch inaktiv geschaltet. Die PIN kann über den Monitor-Menüpunkt "PIN eingeben" somit nicht mehr eingegeben werden. Damit ist sichergestellt, dass erst unmittelbar vor dem Verbindungsaufbau die PIN abgefragt wird und eingegeben werden muss.

Bei Aktivierung dieser Funktion ist damit ausgeschlossen, dass ein unbefugter Benutzer bei bereits eingegebener PIN eine unerwünschte Verbindung aufbaut.

Ebenso wird für die Aktivschaltung der Funktion "PIN ändern" nicht mehr die bereits in anderem Funktionszusammenhang abgeforderte PIN verwendet - wie beim Verbindungsaufbau oder im Verbindungs-Menü "PIN eingeben". Sondern der Menüpunkt "PIN ändern" ist immer selektierbar, und die neue PIN wird unmittelbar nach der Änderung sogleich wieder zurückgesetzt.



Damit ist sichergestellt, dass bei Konfiguration der "PIN-Abfrage bei jedem Verbindungsaufbau" an einem unbeaufsichtigten Client-Monitor zu keinem Zeitpunkt eine bereits eingegebene PIN von einem unbefugten Benutzer für einen Verbindungsaufbau genutzt werden kann.

4.1.9 PIN zurücksetzen

Dieser Menüpunkt kann gewählt werden, um die PIN zu löschen, d.h. um die aktuell gültige PIN für einen anderen Benutzer unbrauchbar zu machen. Dies kann dann sinnvoll sein, wenn der Arbeitsplatz vorübergehend verlassen wird oder wenn der Benutzer gewechselt wird. Danach muss erneut eine gültige PIN eingegeben werden, um eine Authentisierung durchführen zu können.

■ **PIN-Status im Client Monitor**

Wurde die PIN bereits eingegeben, erscheint im Monitor die Einblendung "PIN" mit einem grünen Haken. Wurde die PIN noch nicht korrekt eingegeben, fehlt das Symbol (siehe oben → Statusanzeigen).

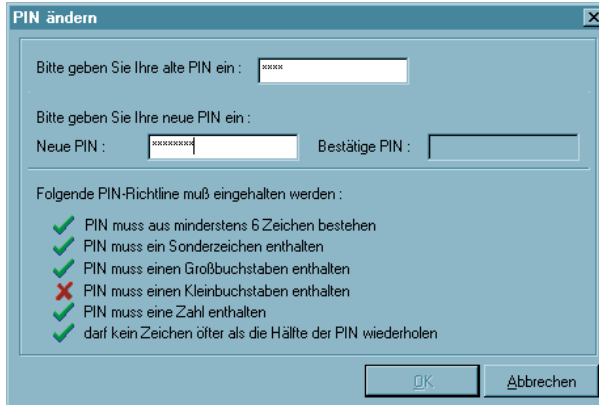
■ **PIN-Eingabezwang nach Abmeldung oder Sleep-Mode**

Wird unter den Betriebssystemen Windows NT/2000/XP der Benutzer gewechselt, wird der PIN-Status zurückgesetzt und die PIN muss erneut eingegeben werden. Wechselt der Computer in den Sleep-Modus, wird ebenfalls der PIN-Status zurückgesetzt.

■ **Anzeige der Meldungen des ACE-Servers für RSA-Token**

Werden vom ACE-Server auf Grund des RSA-Tokens Nachrichten versendet, werden diese am Monitor in einem Eingabefeld angezeigt (z.B. "Ablauf der gültigen PIN").

4.1.10 PIN ändern



Unter diesem Menüpunkt kann die PIN für eine Smart Card oder ein Soft-Zertifikat geändert werden, wenn vorher die richtige PIN eingegeben wurde (siehe → PIN eingeben).

Ohne die vorherige Eingabe einer gültigen PIN wird dieser Menüpunkt nicht aktiviert.

Aus Sicherheitsgründen – um die PIN-Änderung nur für den autorisierten Benutzer zuzulassen –, muss nach Öffnen dieses Dialogs die noch gültige PIN ein zweites Mal eingegeben werden. Die Ziffern der PIN werden in diesem und den nächsten Eingabefeldern als Sterne “*” dargestellt.



Anschließend geben Sie Ihre neue PIN ein und bestätigen diese durch Wiederholung im letzten Eingabefeld. Mit Klick auf “OK” haben Sie Ihre PIN geändert. Die einzuhalten- den PIN-Richtlinien werden unter den Eingabefeldern eingeblendet. Sie können im Hauptmenü unter “Zertifikate → PIN-Richtlinien” eingestellt werden (Bild oben).

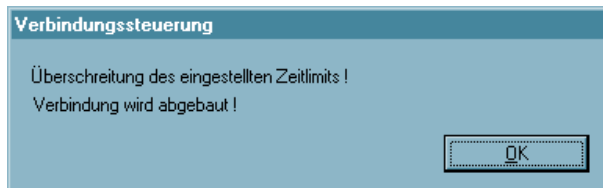
Während der Eingabe einer neuen PIN wird vor die jeweils erfüllten Richtlinien das rote Kreuz durch einen grünen Haken ausgetauscht (Bild oben).

4.1.11 Verbindungssteuerung Statistik

Statistik der Verbindungssteuerung			
	heute	seit 01.04.02	seit 01.01.02
ges. Online-Dauer	0:41:24	0:46:58	0:47:51
ges. Verbindungen	0	0	0
ges. Einheiten	14	25	29
empfangene (KBytes)	0	0	0
gesendete (KBytes)	1	1	1
Hilfe Schließen			

Die Statistik gibt Ihnen Auskunft über Ihre Datenkommunikation. In ihr werden sowohl gesondert als auch aufaddiert die gesamten Online-Zeiten, die gesamte Anzahl der Verbindungen und die gesamten Einheiten, sowie empfangene und gesendete Kbytes für den aktuellen Tag, den laufenden Monat und das laufende Jahr angezeigt.

4.1.12 Sperre aufheben



Je nachdem, wie die Verbindungssteuerung eingestellt ist, erhalten Sie bei Überschreiten eines Limits Meldungen auf dem Bildschirm. Wird ein Limit überschritten und die Verbindung automatisch abgebaut, wird eine Sperre aktiv, die jeden weiteren Verbindungsaufbau unterbindet (siehe → “Verbindung”-Menü im Monitor).

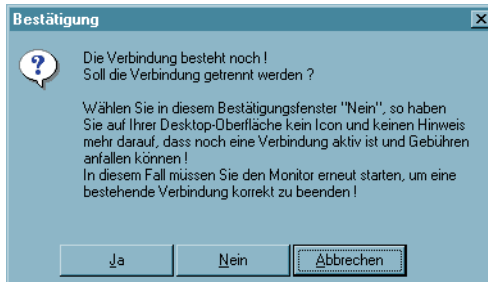
Eine Verbindung kann erst dann wieder neu aufgebaut werden, wenn Sie die “Sperre aufheben”.

4.1.13 Beenden (des Monitors)

Wurde die Verbindung bereits getrennt, beendet ein Klick auf diesen Menüpunkt oder der Schließen-Button den Monitor.

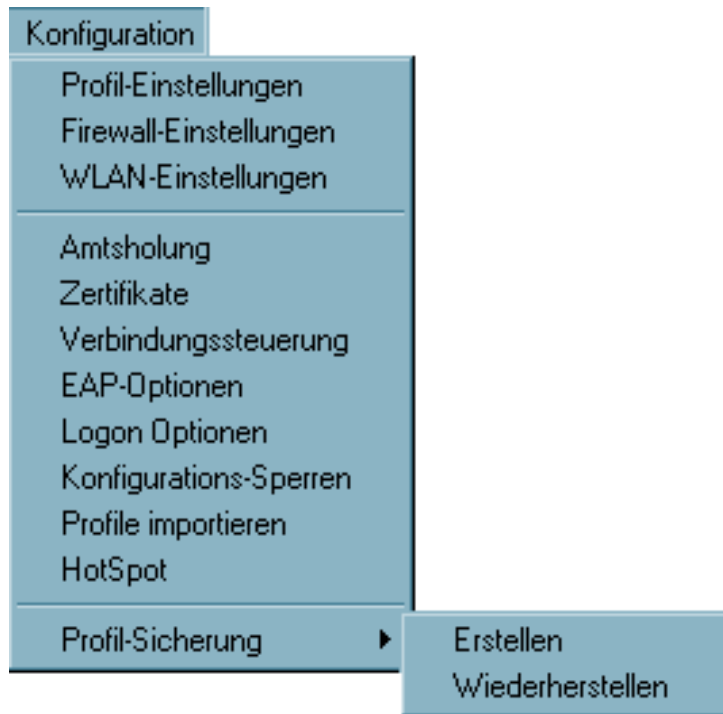


Besteht noch eine Verbindung, kann nach Klick auf diesen Menüpunkt oder den Schließen-Button der Monitor ebenfalls beendet werden. Beachten Sie jedoch unbedingt, dass die Verbindung dabei nicht automatisch getrennt wird. Soll die möglicherweise kostenpflichtige Verbindung bestehen bleiben, obwohl der Monitor beendet wird, so wird dazu ausdrücklich eine Bestätigung von der Software verlangt.



Klicken Sie in diesem Bestätigungsfenster auf "Nein", so haben Sie auf Ihrer Desktop-Oberfläche kein Icon und keinen Hinweis mehr darauf, dass noch eine Verbindung aktiv ist und Gebühren anfallen können! In diesem Fall müssen Sie den Monitor erneut starten, um eine bestehende Verbindung korrekt zu beenden!

4.2 Konfiguration



Unter diesem Menüpunkt können sämtliche Einstellungen für die Arbeit mit dem IPSec Client vorgenommen werden, die länger als eine Session bestehen sollen. Dies betrifft das Anlegen der Profile, die Konfiguration der IPSec-Verbindungen, die Firewall-Einstellungen, sowie die Eingabe einer Amtsholung für Anschlüsse an Telekommunikationsanlagen.

Darüber hinaus kann eigens konfiguriert werden, wie Zertifikate genutzt werden sollen, wie die Verbindungssteuerung arbeiten soll und welche Konfigurations-Rechte der Benutzer erhält.

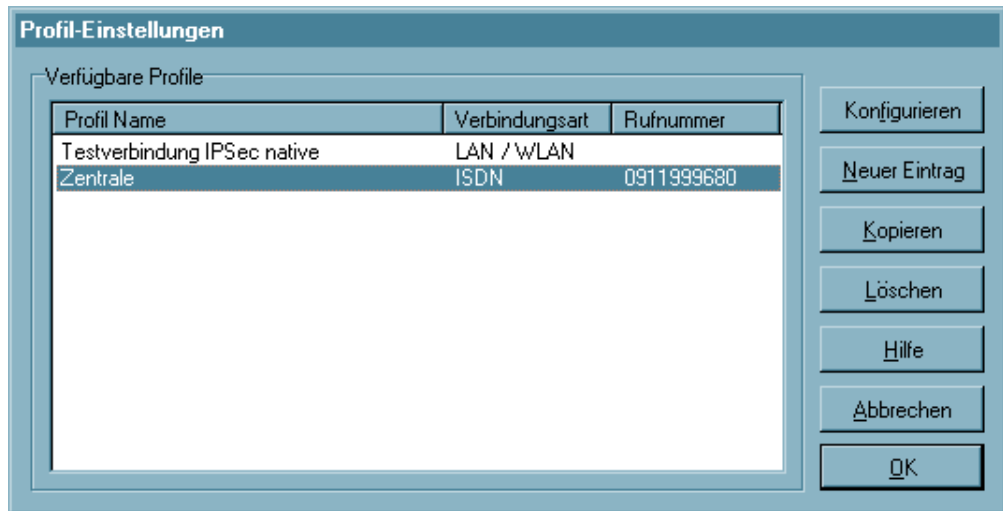
4.2.1 Profil-Einstellungen

■ Die Einträge der Profil-Einstellungen

Bei einer Erstinstallation der IPSec Client Software ist noch kein Profil vorhanden. In diesem Fall wird automatisch ein Konfigurations-Assistent eingeblendet, der Ihnen hilft, eine Konfiguration anzulegen. Damit wird zugleich das erste Profil der IPSec Client Software angelegt. Dieser Assistent wird auch gestartet bei Klick auf “Neuer Eintrag” (siehe unten, “Neuer Eintrag – Profil”).

Mit den Profil-Einstellungen kann die Parametrisierung für die Zielsysteme (Profil) durchgeführt und die Übertragungsart, den Benutzeranforderungen entsprechend, bis ins Detail konfiguriert werden.

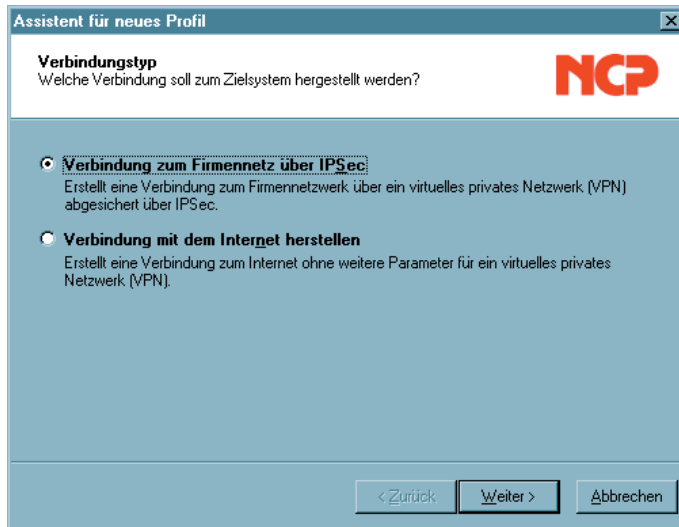
Nachdem Sie auf “Profil-Einstellungen” im Monitor-Menü “Konfiguration” geklickt haben, öffnet sich das Menü und zeigt in einer Liste der bereits verfügbaren Profile deren Namen und die Rufnummern der zugehörigen Zielsysteme.



Auf der rechten Seite der Profil-Einstellungen sind Buttons angebracht zu folgenden Funktionen: Konfigurieren, Neuer Eintrag, Kopieren, Löschen, OK, Hilfe und Abbrechen.

■ Neuer Eintrag – Profil

Um ein neues Profil zu definieren, klicken Sie auf “Profil-Einstellungen”. Wenn sich das Fenster des Menüs öffnet klicken Sie auf “Neuer Eintrag”. Jetzt legt der “Assistent für ein neues Profil” mit Ihrer Hilfe ein neues Profil an. Dazu blendet er die unbedingt notwendigen Parameter auf. Wenn Sie die Einträge in diesen Feldern vorgenommen haben, ist ein neues Profil angelegt. Für alle weiteren Parameterfelder des Profils werden Standardwerte eingetragen.



Mit dem Konfigurations-Assistenten können Verbindungen mit dem Internet oder zum Firmennetz rasch hergestellt werden. Je nach Auswahl des gewünschten Verbindungstyps wird das Profil nach wenigen Konfigurationsabfragen angelegt.

Im folgenden die jeweils nötigen Daten zur Konfiguration:

Verbindung zum Firmennetz über IPsec:

- Profil-Name
- Verbindungsmedium
- Zugangsdaten für Internet-Dienstleister (Benutzername, Passwort, Rufnummer)
- VPN-Gateway-Parameter (Tunnelendpunkt IP-Adresse)
- Zugangsdaten für VPN-Gateway (XAUTH, Benutzername, Passwort)
- IPsec-Konfiguration (Exch. Mode, PFS-Gruppe, Kompression)
- Statischer Schlüssel (Preshared Key), ohne Zertifikat (IKE ID-Typ, IKE ID)
- IP-Adressen-Konfiguration (IP-Adresse des Clients, DNS/WINS-Server)
- Firewall-Einstellungen

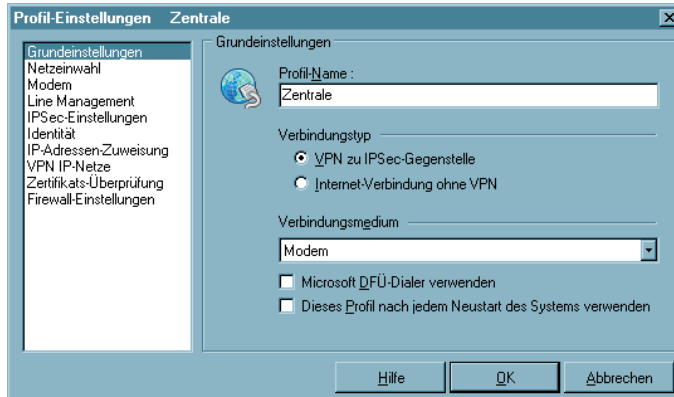
Verbindung mit dem Internet herstellen:

- Profil-Name
- Verbindungsmedium
- Zugangsdaten für Internet-Dienstleister (Benutzer, Passwort, Rufnummer)

Das neue Profil erscheint nun in der Liste der Profile mit dem von Ihnen vergebenen Namen. Wenn keine weiteren Parameter-Einstellungen nötig sind, können Sie die Liste mit Ok schließen. Das neue Profil ist im Monitor sofort verfügbar. Es kann im Monitor ausgewählt werden und über das Menü "Verbindung → Verbinden" kann das zugehörige Ziel sofort angewählt werden.

■ Konfigurieren – Profil

Um die (Standard-)Werte eines Profils zu editieren, wählen Sie mit der Maus das Profil, dessen Werte Sie ändern möchten, und klicken anschließend auf “Konfigurieren”. Die Profil-Einstellungen zeigen nun in ihrem linken Fenster eine Liste von Begriffen, denen jeweils ein Parameterfeld zugeordnet ist:



*Grundeinstellungen
Netzeinwahl
Modem
Line Management
IPSec-Einstellungen
Identität
IP-Adressen-Zuweisung
VPN IP-Netze
Zertifikats-Überprüfung
Firewall-Einstellungen*

Je nachdem, welcher Begriff markiert wird, zeigt sich das entsprechende Feld mit den zugehörigen Parametern (siehe → 4. Konfigurationsparameter).

■ Ok – Profil

Die Konfiguration eines Profils ist abgeschlossen, wenn Sie das Konfigurationsfenster mit “OK” schließen. Das neue oder geänderte Profil ist im Monitor sofort verfügbar. Es kann im Monitor über die Profilauswahl selektiert werden und über das Menü “Verbindung → Verbinden” sofort zur Anwahl an das Zielsystem verwendet werden.

■ Kopieren – Profil

Um die Parameter-Einstellungen eines bereits definierten Profils zu kopieren, markieren Sie das zu kopierende Profil in der Liste und klicken Sie auf den Kopieren-Button. Daraufhin wird das Grundeinstellungen-Parameterfeld geöffnet. Ändern Sie nun den Eintrag in “Profil-Name” und klicken Sie anschließend Ok. Nur wenn Sie den Namen des Profils ändern, kann es auch als neuer Eintrag in der Liste der Profile vermerkt werden.



Ein kopiertes Profil muss einen neuen, noch nicht vergebenen, Namen erhalten. Nur so kann es in der Liste der Profile abgelegt werden.

■ Löschen – Profil

Um ein Profil zu löschen, wählen Sie es aus und klicken den Löschen-Button.

4.2.2 Firewall-Einstellungen

Alle Firewall-Mechanismen sind optimiert für Remote Access-Anwendungen und werden bereits beim Start des Rechners aktiviert. D.h. im Gegensatz zu VPN-Lösungen mit eigenständiger Firewall ist der Telearbeitsplatz bereits vor der eigentlichen VPN-Nutzung gegen Angriffe geschützt.

Die Firewall bietet auch im Fall einer Deaktivierung der Client-Software vollen Schutz des Endgerätes.



Bitte beachten Sie, dass die Firewall-Einstellungen global, d.h. für alle Zielsysteme des Telefonbuchs gültig sind.



Dagegen ist die Einstellung der Link Firewall, die im Telefonbuch vorgenommen werden kann, nur für den dazu gehörenden Telefonbuch-Eintrag (Zielsystem) und die Verbindung zu diesem Zielsystem wirksam.

Eigenschaften der Firewall

Die Firewall arbeitet nach dem Prinzip der Paketfilterung in Verbindung mit Stateful Packet Inspection (SPI). Die Firewall prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis des konfigurierten Regelwerks, ob ein Datenpaket weitergeleitet oder verworfen wird.

Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen wird der unbefugte Zugriff auf Daten und Ressourcen im zentralen Datennetz verhindert. Zum anderen wird mittels Stateful Inspection der jeweilige Status bestehender Verbindungen überwacht. Die Firewall kann darüber hinaus erkennen, ob eine Verbindung "Tochterverbindungen" geöffnet hat – wie beispielsweise bei FTP oder Netmeeting – deren Pakete ebenfalls weitergeleitet werden müssen. Wird eine Regel für eine ausgehende Verbindung definiert, die einen Zugriff erlaubt, so gilt die Regel automatisch für entsprechende Rückpakete. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf.

Die Firewall-Regeln können dynamisch konfiguriert werden, d.h. ein Anhalten der Software oder ein Reboot ist nicht nötig.

Die Firewall-Einstellungen im Konfigurationsmenü des Client-Monitors gestatten eine genauere Spezifikation von Firewall-Filterregeln. Sie wirken global. D.h. unabhängig vom aktuell gewählten Zielsystem werden immer zuerst die Regeln der erweiterten Firewall-Einstellungen abgearbeitet, bevor die Regeln der Firewall aus dem Telefonbuch angewendet werden.

Eine Kombination der globalen und link-bezogenen Firewall kann in bestimmten Szenarien durchaus sinnvoll sein. Im Allgemeinen sollten jedoch nahezu alle Anforderungen über die globalen Einstellungsmöglichkeiten abzudecken sein.

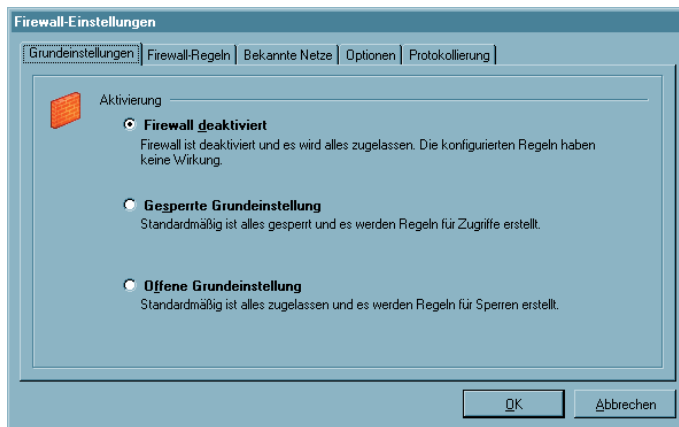
Bitte beachten Sie, dass die link-bezogenen Firewall-Einstellungen bei Aktivierung Vorrang den globalen haben. Ist z.B. die Link-Firewall auf "immer" und "Ausschließlich Kommunikation im Tunnel zulassen" eingestellt, kann trotz evtl. anders lautender Regeln der globalen Konfiguration nur ein Tunnel aufgebaut und darüber kommuniziert werden. Jeglicher anderer Verkehr wird von der Link-Firewall verworfen.

Konfiguration der Firewall-Einstellungen

Die Filterregeln der erweiterten Firewall können sowohl anwendungsbezogen als auch (zusätzlich) adressorientiert, bezüglich bekannter/unbekannter Netze, definiert werden.

Um Konflikte zwischen den Regeln der verbindungsorientierten Firewall des Telefonbuchs und der erweiterten Firewall zu vermeiden, wird empfohlen, die Firewall des Telefonbuchs auf "inaktiv" zu schalten, wenn die erweiterte Firewall eingesetzt wird. Die IP-Adressen der jeweiligen Verbindung (zum Ziel-Gateway) können stattdessen in den Filterregeln der erweiterten Firewall eingesetzt werden.

Konfigurationsfeld Grundeinstellungen



In den Grundeinstellungen wird festgelegt, mit welcher Basis-Policy die Firewall arbeiten soll.

Firewall deaktiviert

Wird die erweiterte Firewall deaktiviert, so wird in diesem Kompatibilitätsmodus nur die im Telefonbuch konfigurierte Firewall genutzt. Dies bedeutet, dass alle Datenpakete nur über die Sicherheitsmechanismen dieser verbindungsorientierten Firewall abgearbeitet werden.

Gesperrte Grundeinstellung (empfohlen)

Wird diese Einstellung gewählt, so sind die Sicherheitsmechanismen der Firewall immer aktiv. D. h. ohne zusätzlich konfigurierte Regeln wird jeglicher IP-Datenverkehr unterbunden. Ausgenommen sind die Datenpakete, die durch eigens erstellte, aktive Firewall-Regeln gestattet (durchgelassen) werden (Permit Filter). Trifft eine der Eigenschaften eines Datenpakets auf die Definition einer Firewall-Regel zu, wird an dieser Stelle die Abarbeitung der Filterregeln beendet und das IP-Paket weitergeleitet.

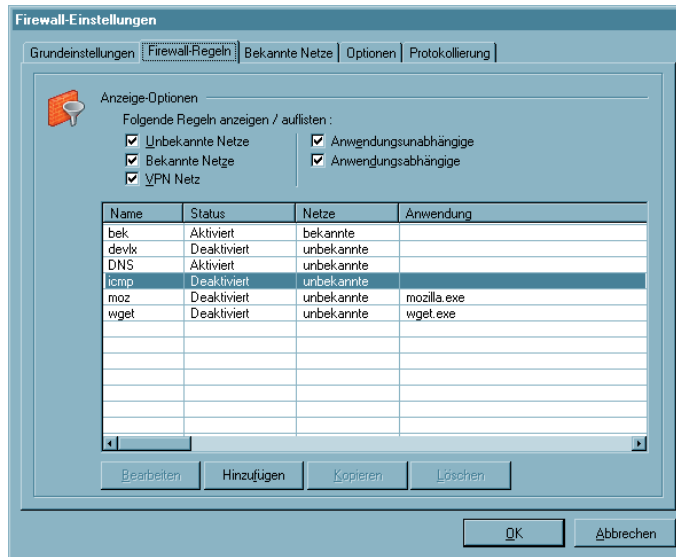
Im Modus der gesperrten Grundeinstellung kann auf komfortable Weise eine IPSec-Tunnelkommunikation freigeschaltet werden. Hierbei kann unter "Optionen" der Datenverkehr über das VPN-Protokoll IPSec global zugelassen werden.

Offene Grundeinstellung

In der offenen Grundeinstellung sind zunächst alle IP-Pakete zugelassen. Ohne weitere Filterregeln werden alle IP-Pakete weitergeleitet.

Ausgenommen sind die Datenpakete, die durch eigens erstellte, aktive Firewall-Regeln ausgefiltert (nicht durchgelassen) werden (Deny Filter). Trifft eine der Eigenschaften eines beim Server/Client ankommenden IP-Pakets auf die Definition eines Deny-Filters zu, wird an dieser Stelle die sequentielle Abarbeitung der Filterregeln beendet und das IP-Paket von der Weiterleitung ausgeschlossen. Daten-Pakete, die auf keinen passenden Deny-Filter treffen, werden weitergeleitet.

■ Konfigurationsfeld Firewall-Regeln



In diesem Konfigurationsfenster werden die Regeln für die Firewall zusammengestellt. Die Anzeige-Optionen sind standardmäßig alle aktiv. Mittels dieser wird eingestellt, welche Regeln in Abhängigkeit ihrer Zuordnung in der Übersicht angezeigt werden:

- unbekannte Netze
- bekannte Netze
- VPN-Netze
- anwendungsabhängig,
- unabhängig

Diese Auswahlfelder für die Anzeigen der Regeln dienen nur der Übersichtlichkeit und haben keine Auswirkung auf die Anwendung einer Filterregel. Für jede definierte Regel werden die wichtigsten Eigenschaften gezeigt:

- Name
- Status
- Netz
- Anwendung

Durch Klick auf diese Eigenschafts-Buttons können die eingeblendeten Regeln sortiert werden.

Erstellen einer Firewall-Regel

Über die Buttons unterhalb der Anzeigezeilen werden die Regeln erzeugt oder bearbeitet. Um eine Firewall-Regel zu erstellen, klicken Sie auf "Hinzufügen". Die Erstellung einer Filterregel erfolgt über vier Konfigurationsschritte bzw. Registerkarten:

- Allgemein: In diesem Konfigurationsfeld wird festgelegt für welche Netze und welches Protokoll die Regel gelten soll.
- Lokal: In diesem Konfigurationsfeld werden die Werte der lokalen Ports und IP-Adressen eingetragen.
- Remote: Im Remote-Feld werden die Port- und Adress-Werte der Gegenseite eingetragen.
- Anwendungen: In diesem Konfigurationsfeld kann die Regel einer oder mehrerer Anwendungen zugeordnet werden.

■ Firewall-Regel / Allgemein

Firewall-Regel

Allgemein | Lokal | Remote | Anwendungen

Name der Regel:

Status:

Richtung:

Die Regel soll für folgende Netze angewendet werden:

☐ Unbekannte Netze

☐ Bekannte Netze

☐ VPN Netze

Protokoll:

OK Abbrechen

Einzelregeln stellen immer Ausnahmen von der Grundeinstellung dar (siehe → Grundeinstellung).

Name der Regel

Mit diesem Namen erscheint die Regel in der Anzeigeliste.

Status

Die Regel wird nur dann auf Datenpakete angewendet, wenn der Status "aktiv" ist.

Richtung

Mit der Richtung geben Sie an, ob diese Regel für eingehende oder ausgehende Datenpakete gelten soll. Wird die Richtung auf ausgehend gesetzt, wird nach dem Prinzip von Stateful Inspection gearbeitet (siehe → Eigenschaften der Firewall). Stateful Inspection wird jedoch nur für die Protokolle UDP und TCP angewendet. Auf "eingehend" kann z.B. dann geschaltet werden, wenn von Remote-Seite eine Verbindung aufgebaut werden soll (z.B. für "eingehende Rufe" oder Administrator-Zugriffe). Die Einstellung "bidirektional" ist nur sinnvoll, wenn Stateful Inspection nicht zur Verfügung steht, z.B. für das ICMP-Protokoll (bei einem Ping).

Die Regel soll für folgende Netze angewendet werden

Beim Neuanlegen einer Regel ist diese zunächst keinem Netz zugeordnet. Eine Regel kann erst dann gespeichert werden, wenn die gewünschte Zuordnung erfolgt ist und ein Name vorgegeben wurde.

Unbekannte Netze

– sind alle Netze (IP-Netzwerkschnittstellen), die weder einem bekannten noch einem VPN-Netz zugeordnet werden können. Darunter fallen z.B. Verbindungen über das DFÜ-Netzwerk von Microsoft oder auch direkte und unverschlüsselte Verbindungen mit dem integrierten Dialer des Clients, wie auch HotSpot WLAN-Verbindungen. Soll eine Regel für unbekannte Netze gelten, so muss diese Option aktiviert werden.

Bekannte Netze

– werden im gleichnamigen Register im Fenster “Firewall-Einstellungen” definiert. Sollte eine Regel für bekannte Netze gelten, muss diese Option aktiviert werden.

VPN-Netze

– sind alle IPSec-Verbindungen in aufgebautem Zustand. Darüber hinaus fallen unter diese Gruppe auch alle verschlüsselten Direktwahlverbindungen über den integrierten Dialer des Clients. Sollte eine Regel für VPN-Netze gelten, so muss diese Option aktiviert werden.

Protokoll

Je nach Anwendung oder Art der Verbindung ist das entsprechende Protokoll zu wählen:

TCP, UDP, ICMP, GRE, ESP, AH, IGRP, RSVP, IPv6 oder IPv4, Alle

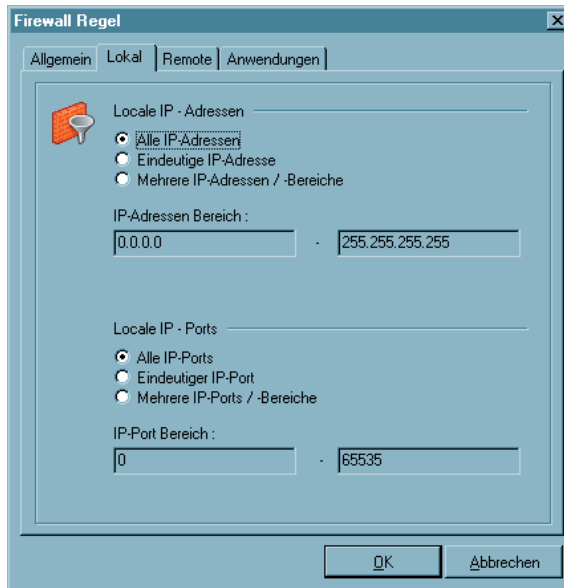
Verbindungssteuerung

Über diese Parameter wird die Art der Verbindung beeinflusst.

Sie wählen z. B. die Option, dass die hier konfigurierte Regel “nur gültig bei inaktiver VPN-Verbindung” ist, wenn Sie wünschen, dass z.B. eine Internet-Verbindung bei gleichzeitig bestehender VPN-Verbindung ausgeschlossen wird, ansonsten aber Internet-Verbindungen zu unbekannten Netzen zugelassen sein sollen. Dazu muss diese Regel für “unbekannte Netze” angewendet werden, d.h. diese Regel muss den Zugang zu unbekannten Netzen zulassen.

Die Option “kein automatischer Verbindungsaufbau” steht nur bei gesperrter Grundeinstellung zur Verfügung. Sie ist nur sinnvoll, wenn im Telefonbuch im Parameterfeld “Verbindungssteuerung” der Verbindungsaufbau auf “automatisch” gestellt wurde. Für die über diese Regel definierten Datenpakete findet bei Aktivierung dieser Funktion kein automatischer Verbindungsaufbau statt, für andere Datenpakete schon.

■ Firewall-Regel / Lokal



Auf dieser Registerkarte werden die Filter für die lokalen IP-Adressen und IP-Ports eingestellt.

Bei gesperrter Grundeinstellung werden diejenigen Datenpakete von der Firewall nach außen durchgelassen, deren Quelladresse (Source Address) mit der unter "Lokale IP-Adressen" übereinstimmt oder im Gültigkeitsbereich liegt. Von den eingehenden Datenpaketen werden diejenigen durchgelassen, deren Zieladresse (Destination Address) mit der unter "Lokale IP-Adressen" übereinstimmt oder im Gültigkeitsbereich liegt.

Ebenso verhält es sich bei gesperrter Grundeinstellung mit den IP-Ports. Diejenigen Datenpakete werden nach außen gelassen, deren Quell-Port (Source Port) unter die Definition der lokalen Ports fällt. Von den eingehenden Datenpaketen werden die durchgelassen, deren Ziel-Port (Destination Port) unter die Definition der lokalen Ports fällt.

Alle IP-Adressen

– umfasst alle Quell-IP-Adressen abgehender bzw. Ziel-IP-Adressen eingehender Pakete, unabhängig vom lokalen Netzwerkadapter.

Eindeutige IP-Adresse

– ist die für den lokalen Netzwerkadapter definierte IP-Adresse. Sie kann je nach Verbindung z.B. der Adresse der Ethernet-Karte, der WLAN-Karte oder auch dem VPN-Adapter zugeordnet sein.

Mehrere IP-Adressen

– bezeichnet einen Adressbereich oder Pool. Z.B. kann dies der IP-Adress-Pool sein, aus dem die vom DHCP Server an den Client zugewiesene Adresse stammt.

Alle Ports

– erlaubt Kommunikation über alle Quellports bei ausgehenden und Ziel-Ports bei eingehenden Paketen.

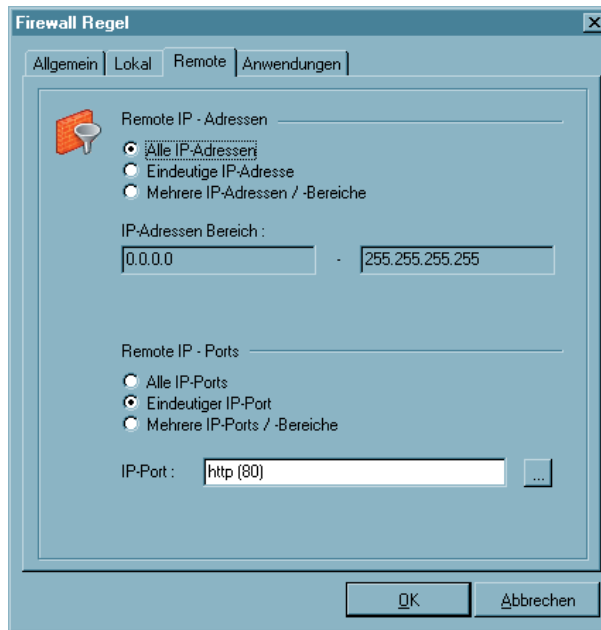
Eindeutiger Port

– Diese Einstellung sollte nur dann verwendet werden, wenn dieses System einen Server-Dienst zur Verfügung stellt (z.B. Remote Desktop auf Port 3389).

Mehrere Ports

– Diese Einstellung sollte nur dann verwendet werden, wenn sich die lokalen Ports zu einem Bereich zusammenfassen lassen, die von einem Dienst benötigt werden, der auf diesem System zur Verfügung gestellt wird (z.B. FTP Ports 20/21).

■ Firewall-Regel / Remote



Auf dieser Registerkarte werden die Filter für die remote IP-Adressen und IP-Ports eingestellt.

Bei gesperrter Grundeinstellung werden diejenigen Datenpakete von der Firewall nach außen durchgelassen, deren Zieladresse (Destination Address) mit der unter "Lokale IP-Adressen" übereinstimmt oder im Gültigkeitsbereich liegt. Von den eingehenden Datenpaketen werden diejenigen durchgelassen, deren Quelladresse (Source Address) mit der unter "Lokale IP-Adressen" übereinstimmt oder im Gültigkeitsbereich liegt.

Ebenso verhält es sich bei gesperrter Grundeinstellung mit den IP-Ports. Diejenigen Datenpakete werden von der Firewall nach außen gelassen, deren Ziel-Port (Destination Port) unter die Definition der lokalen Ports fällt. Von den eingehenden Datenpaketen werden die durchgelassen, deren Quell-Port (Source Port) unter die Definition der lokalen Ports fällt.

Mit den Einstellungen unter Remote-IP-Adressen lässt sich festlegen, mit welchen entfernten IP-Adressen das System kommunizieren darf.

Alle IP-Adressen

– erlaubt die Kommunikation mit beliebigen IP-Adressen der Gegenseite, ohne Einschränkung.

Eindeutige IP-Adresse

– lässt nur Kommunikation mit der hier angegebenen IP-Adresse auf der Gegenseite zu.

Mehrere IP-Adressen / -Bereiche

– gestattet die Kommunikation mit verschiedenen IP-Adressen auf der Gegenseite entsprechend der Einträge.

Mit den Einstellungen unter Remote Ports lässt sich festlegen, über welche Ports mit entfernten Systemen kommuniziert werden darf.

Alle Ports

– setzt keinerlei Beschränkungen hinsichtlich Ziel-Port bei abgehenden bzw. Quell-Port bei eingehenden Paketen.

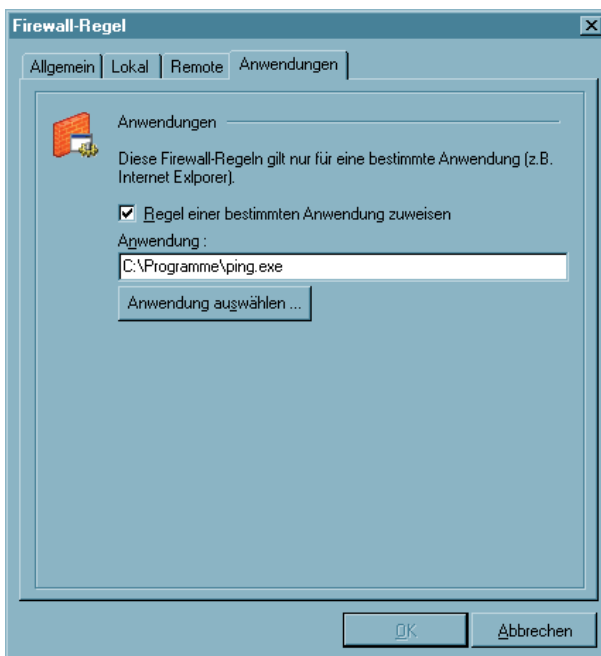
Eindeutiger Port

– lässt nur eine Kommunikation über den angegebenen Port zu, wenn dieser als Ziel-Port im abgehenden bzw. als Quell-Port im eingehenden Paket vorkommt. Soll z.B. eine Regel nur Telnet zu einem anderen System zulassen, ist hier Port 23 einzutragen.

Mehrere Ports / Bereiche

– können verwendet werden, wenn mehrere Ports für eine Regel verwendet werden sollen (z.B. FTP Port 20/21).

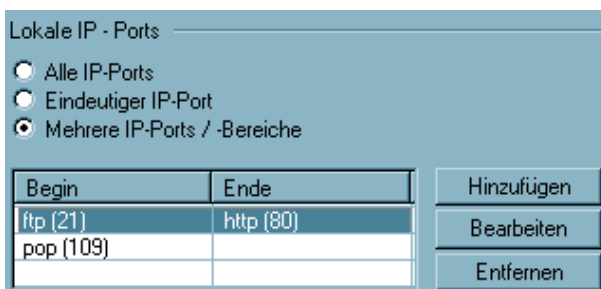
■ Firewall-Regel / Anwendungen



Regel einer bestimmten Anwendung zuweisen

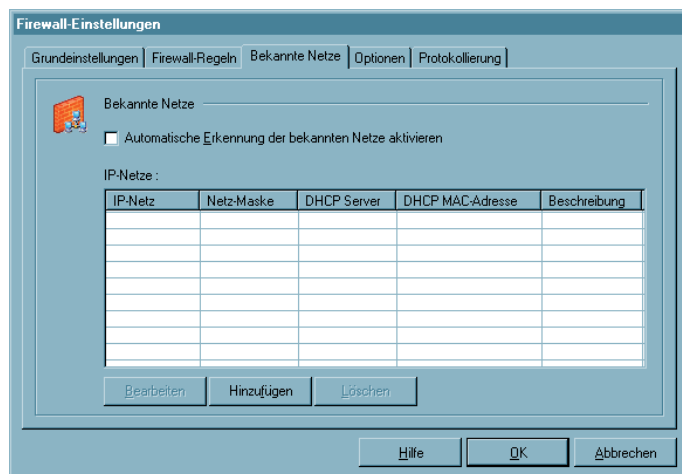
– besagt, dass (bei gesperrter Grundeinstellung) für diese Anwendung eine Verbindung möglich ist. Wird über den Button “Anwendung auswählen” eine lokal installierte Anwendung, wie z.B. ping.exe, selektiert, so kann nur diese Applikation kommunizieren. In diesem Fall dürfen nach dieser Regel nur Pings ausgeführt werden.

In diesem Beispiel sollte dann auch beachtet werden, dass vom Protokoll her ICMP zugelassen ist.



Beachten Sie, dass auch der zugehörige Port selektiert sein muss. Für eine E-Mail-Anwendung (80).

Konfigurationsfeld Bekannte Netze



Wurde im Konfigurationsfeld “Firewall-Regeln” definiert, dass eine Regel auf Verbindungen mit bekannten Netzen (Friendly Nets) anzuwenden ist, so wird diese Regel immer angewendet, wenn ein Netz nach den hier anzugebenden Kriterien als Friendly Net identifiziert werden kann, bzw. der LAN-Adapter sich in einem Friendly Net befindet.

Der LAN-Adapter des Clients befindet sich dann in einem Friendly Net wenn:

[IP-Netze und Netzmaske]

– die IP-Adresse des LAN-Adapters aus dem angegebenen Netzbereich stammt. Ist z.B. das IP-Netz 192.168.254.0 mit der Maske 255.255.255.0 angegeben, so würde die Adresse 192.168.254.10 auf dem Adapter eine Zuordnung zum bekannten Netz bewirken.

[DHCP Server]

– diese IP-Adresse von dem DHCP Server zugewiesen wurde, der die hier angegebene IP-Adresse besitzt;

[DHCP MAC-Adresse]

– wenn dieser DHCP Server die hier angegebene MAC-Adresse besitzt. Diese Option kann nur dann verwendet werden, wenn sich der DHCP Server im selben IP-Subnet befindet wie der DHCP Client.

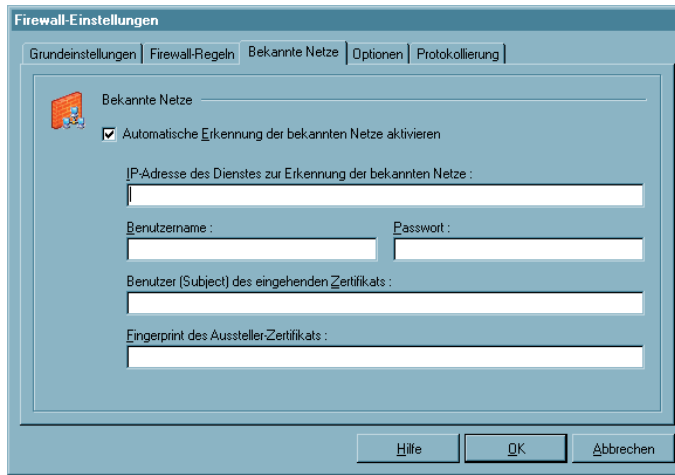
Je mehr dieser Bedingungen erfüllt werden, desto präziser ist der Nachweis, dass es sich um ein vertrautes Netz handelt.

Die Zuordnung eines Adapters zu unbekannten oder bekannten Netzen wird automatisch protokolliert im Log-Fenster des Client-Monitors und in der Log-Datei der Firewall (siehe → Protokollierung), wenn dieser DHCP Server die hier angegebene MAC-Adresse besitzt.

Automatische Erkennung der bekannten Netze aktivieren

Zur automatischen Friendly Net Detection beachten Sie bitte das Parameterfeld auf der folgenden Seite.

■ Automatische Erkennung der bekannten Netze



Was ein Friendly Net ist, wird vom Administrator zentral verbindlich festgelegt. Die Signalisierung eines Friendly Net erfolgt im Monitor durch das Firewall-Symbol, das sich grün färbt, sobald sich der Client in ein Friendly Net eingewählt hat.

IP-Adresse des Dienstes zur Erkennung der bekannten Netze

Erforderlich ist ein Friendly Net Detection Server (FNDS), d.h. eine Softwarekomponente von NCP, in einem als "Friendly Net" definierten Netz. Dieser FND Server muss über IP erreichbar sein und seine IP-Adresse hier eingetragen werden. Die Adresse eines zweiten Servers kann als Ersatz nach einem Semikolon eingetragen werden.

Benutzername, Passwort (FNDS)

Die Authentisierung des Friendly Net Detection Servers erfolgt über MD5 oder TLS. Hier einzutragender Benutzername und Passwort müssen mit jenen am FNDS hinterlegten übereinstimmen.

Benutzer (Subject) des eingehenden Zertifikats

Das eingehende Zertifikat des FNDS wird auf diesen String hin geprüft. Nur bei Gleichheit handelt es sich um ein Friendly Net.

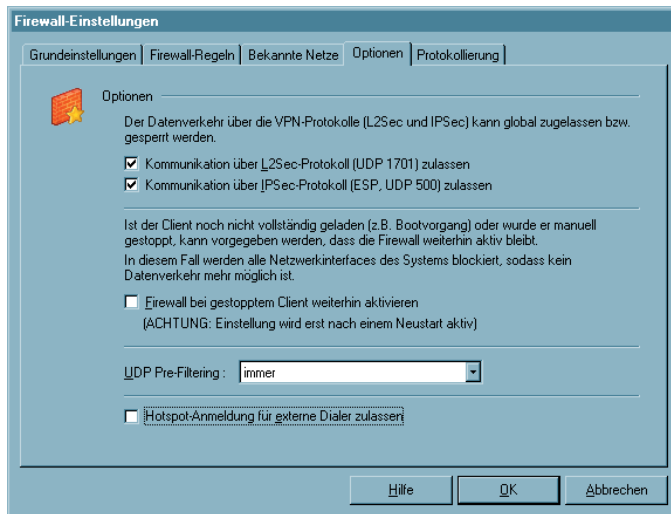
Fingerprint des Aussteller-Zertifikats

Um ein Höchstmaß an Fälschungssicherheit bieten zu können, muss der Fingerprint des Aussteller-Zertifikats überprüft werden können. Er muss mit dem hier eingegebenen Hash-Wert übereinstimmen.

Friendly Net Detection mittels TLS

Soll die Friendly Net Detection mittels TLS erfolgen (einschließlich einer Authentisierung über den Fingerprint des Aussteller-Zertifikats), so muss sich im Programmverzeichnis "CaCerts" obiges Aussteller-Zertifikat befinden und dessen Fingerprint muss mit dem hier konfigurierten übereinstimmen.

Konfigurationsfeld Optionen



Bei gesperrter Grundeinstellung kann der Aufbau von VPN-Verbindungen über dieses Register global zugelassen werden. Folgende für den Tunnelaufbau benötigten Protokolle und Ports werden per automatisch generierter Filter freigegeben:

Für IPSec:
 UDP 500 (IKE
 ISAKMP), IP-Protokoll
 50 (ESP), UDP 4500
 (NAT-T),
 UDP 67 (DHCPs),
 UDP 68 (DHCPc)

Diese globale Definition erspart die Einrichtung dedizierter Einzelregeln für die jeweilige VPN-Variante.



Bitte beachten Sie, dass dadurch lediglich der Tunnelaufbau ermöglicht wird. Existieren keine weiteren Regeln für VPN-Netze, die eine Kommunikation im Tunnel zulassen, kann über die VPN-Verbindung kein Datenaustausch erfolgen.

Firewall bei gestopptem Client weiterhin aktivieren

Die Firewall kann auch bei gestopptem Client aktiv sein, wenn diese Funktion selektiert wird. In diesem Zustand wird jedoch jede ein- und ausgehende Kommunikation unterbunden, so dass keinerlei Datenverkehr möglich ist, solange der Client deaktiviert ist. Wird oben genannte Funktion nicht genutzt und der Client gestoppt, so wird auch die Firewall deaktiviert.

UDP Pre-Filtering

In der Standardeinstellung werden bei gestartetem Client (unabhängig von der Firewall) UDP-Pakete ausgefiltert, so dass eine Verbindung von außen zum Client PC nicht möglich ist. Ist auf dem Client PC eine Anwendung mit Server-Funktion gestartet, die auf UDP-Datentransfer basiert (wie z. B. Terminalanwendungen oder NTP), kann sich diese Standardeinstellung störend auf die Datenkommunikation auswirken. Daher kann diese Standardeinstellung ausgeschaltet oder auf die UDP-Pakete unbekannter Netze beschränkt werden.

immer: Standardeinstellung. In dieser Schalterstellung gelangen bei gestartetem Client keine UDP-Pakete auf den Client PC.

nur bei unbekannten Netzen: In dieser Schalterstellung wirkt der UDP-Filter nur auf Pakete, die über Adapter unbekannter Netze eintreffen.

aus: Wird der Filter ausgeschaltet, gelangen alle UDP-Pakete auf den Client PC. Diese Einstellung sollte nur verwendet werden, wenn Probleme mit einer Anwendung auftreten.

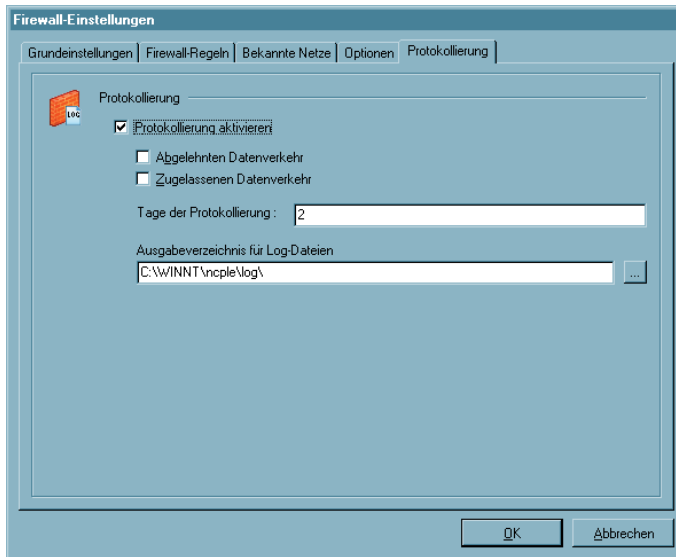
HotSpot-Anmeldung für externe Dialer zulassen

Wenn diese Funktion aktiviert ist, kann über einen externen Dialer eine HotSpot-Anmeldung erfolgen. Dazu wird die Kommandozeilen-schnittstelle `rwscmd.exe` aufgerufen. (Beachten Sie dazu die Beschreibung im Anhang "Services" in diesem Handbuch!) Mit dem Befehl

```
rwscmd /logonhotspot [Timeout]
```

wird die Firewall für die Ports 80 (HTTP) und 443 (HTTPS) freigeschaltet. Damit wird eine dynamische Regel erzeugt, die den Datenverkehr zulässt, bis der übergebene Timeout (in Sekunden) abgelaufen ist.

Konfigurationsfeld Protokollierung



Die Aktivitäten der Firewall werden je nach Einstellung in eine Log-Datei geschrieben. Das “Ausgabeverzeichnis für Log-Dateien” befindet sich standardmäßig im Installationsverzeichnis unter LOG\.

Die Log-Dateien für die Firewall sind im reinen Textformat geschrieben und benannt als Firewallyymmdd.log. Sie beinhalten eine Beschreibung vom “abgelehnten Datenverkehr” und/oder “zugelassenen Datenverkehr”. Wurde keine dieser Optionen selektiert, so werden nur Statusinformationen zur Firewall hinterlegt.

Die Log-Dateien werden bei jedem Start der Firewall geschrieben. Maximal werden davon so viele im Log-Verzeichnis gehalten, wie als Anzahl der “Tage der Protokollierung” eingegeben wurde.

4.2.3 WLAN-Einstellungen

Integrierte WLAN-Konfiguration für Windows 2000/XP

In diesem Konfigurationsmenü “Konfiguration / WLAN-Einstellungen” können die Zugangsdaten zum Funknetz in einem Profil hinterlegt werden. (Dieses Konfigurationsfeld kann unabhängig vom aktuell selektierten Linkprofil auch über das Monitormenü “Fenster / WLAN-Status anzeigen” geöffnet werden.)

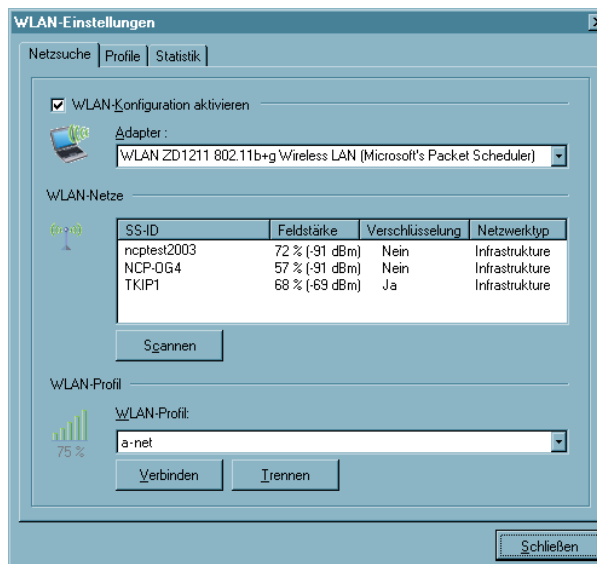
WLAN-Automatik

Unter “WLAN-Profil” wird das Profil selektiert, über das eine Verbindung zum Access Point hergestellt werden soll. Außer diesem Profil können automatisch noch weitere Profile zur Anwahl an den Access Point verwendet werden, wenn diese mit Verbindungsart “automatisch” konfiguriert wurden (siehe übernächste Seite) und in den “WLAN-Einstellungen” die Funktion “Für Verbindungsaufbau Profile mit automatischer Verbindungsart verwenden” aktiviert wird.

D. h. wurden mehrere Profile mit der Verbindungsart “automatisch” angelegt und wird die Funktion “Für Verbindungsaufbau Profile mit automatischer Verbindungsart verwenden” genutzt, so wird zunächst das zuletzt selektierte Profil für einen möglichen Verbindungsaufbau herangezogen. Ist die SSID nicht passend, sodass mit diesem Profil keine Verbindung zum Access Point hergestellt werden kann, so werden anschließend die als “automatisch” konfigurierten Profile für den Verbindungsaufbau herangezogen und das mit der passenden SSID verwendet.



Netzsuche



Wird diese “WLAN-Konfiguration aktiviert”, so muss das Management-Tool der WLAN-Karte deaktiviert werden. (Alternativ kann auch das Management-Tool der WLAN-Karte oder das Microsoft-Tool genutzt werden, dann müssen die jeweils nicht eingesetzten Tools deaktiviert werden.)

Adapter

Sofern ein WLAN-Adapter installiert ist, wird dieser angezeigt.

WLAN-Netze

Nach einem automatischen Scan-Vorgang von wenigen Sekunden, der manuell auch mit dem Button “Scannen” ausgelöst werden kann, werden die derzeit verfügbaren Netze mit den Daten zu SS-ID, Feldstärke, Verschlüsselung und Netzwerktyp angezeigt. In einem zugehörigen Profil müssen diese Werte entsprechend konfiguriert werden:

SS-ID

Feldstärke

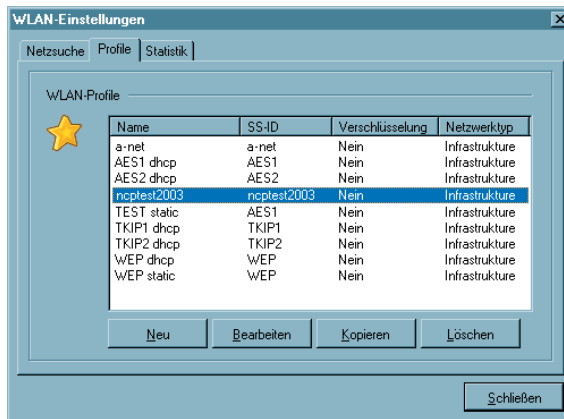
Verschlüsselung

Netzwerktyp

Der Name für die SS-ID (Standard Security) wird vom Netzbetreiber vergeben und unter dem grafischen Feld des Monitors im WLAN-Panel ebenso angezeigt wie die Feldstärke (Bild unten). Die SS-ID wird nach einem Doppelklick auf das zu wählende Netz (z. B. WLAN) automatisch in ein WLAN-Profil für diesen Adapter übernommen wenn zu diesem Netz noch kein Profil erstellt wurde (siehe unten → WLAN-Profile / Allgemein.)



WLAN-Profile

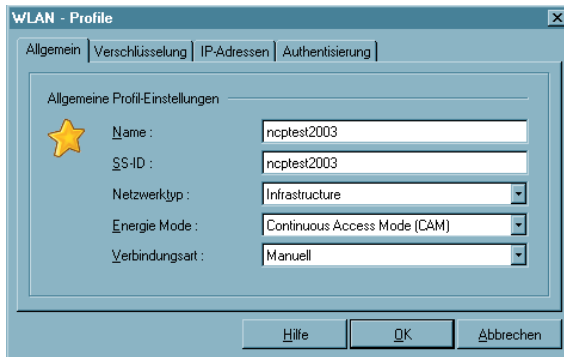


Bereits erstellte Profile zum oben selektierten Adapter werden in einer Liste dargestellt. Netzwerktyp, Verschlüsselung und SS-ID müssen mit den obigen Netzwerkparametern übereinstimmen.

Ein neues Profil wird erzeugt, indem der Button “Neu” gedrückt wird oder im vorigen Fenster auf das zugehörige Netz ein Doppelklick ausgeübt oder die rechte Maustaste geklickt wird. Über die Buttons können Profile auch bearbeitet oder gelöscht werden.

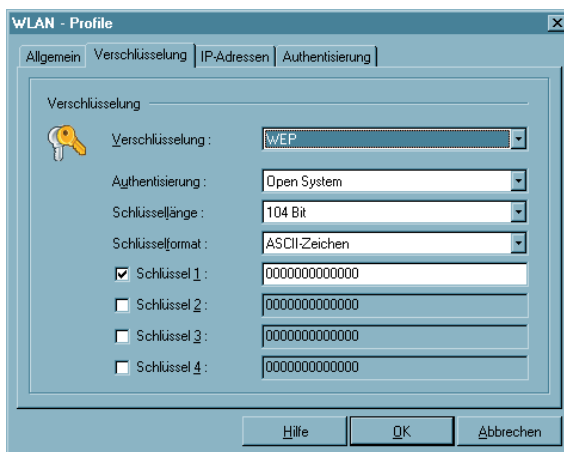
Allgemeine Profil-Einstellungen

Der Name kann frei vergeben werden und ist bei einer neuen Profilerzeugung nach Doppelklick auf das gescannte Netz zunächst identisch mit der SS-ID dieses Netzes. Ebenso verhält es sich mit dem Netzwerktyp, der identisch sein muss mit dem im Broadcast des Funknetzes gesendeten.



Der Netzwerktyp muss dann manuell auf “Ad-Hoc” umgestellt werden, wenn ein Profil für eine Direktverbindung von PC zu PC hergestellt werden soll. Sofern der WLAN-Adapter dies gestattet, kann der Energie Mode für ihn ausgewählt werden.

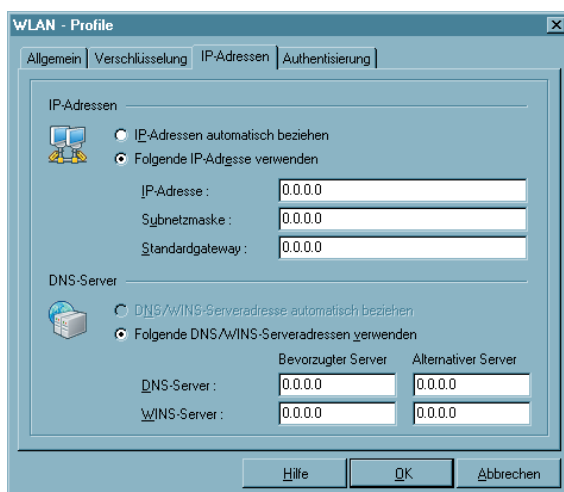
Wird die Verbindungsart für ein selektiertes Profil auf automatisch gestellt, so kann dieses Profil für die WLAN-Automatik (siehe oben) verwendet werden.



Verschlüsselung

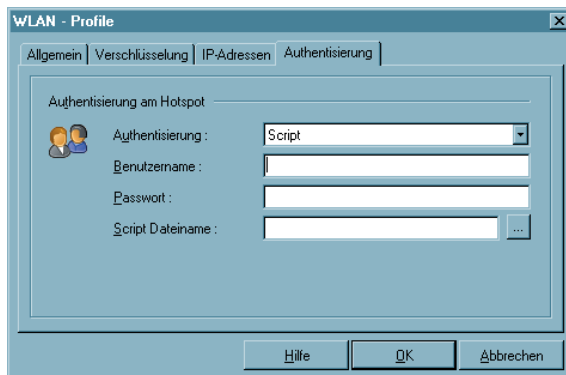
Der Verschlüsselungsmechanismus wird vom Access Point (WLAN Router) vorgegeben und über den Administrator mitgeteilt.

Wird WPA mit EAP (TLS) genutzt, so müssen die EAP-Optionen im Konfigurations-Menü des Monitors aktiviert werden und ein Zertifikat konfiguriert sein (im Monitor-Menü unter “Konfiguration / Zertifikate”).



IP-Adressen

Die hier gemachten Einstellungen zur IP-Adress-Konfiguration der WLAN-Karte werden dann wirksam, wenn die WLAN-Konfiguration wie oben beschrieben aktiviert wurde. In diesem Fall wird die hier eingetragene Konfiguration in die Microsoft-Konfiguration der Netzwerkverbindungen übernommen. (Siehe dort → Netzwerkverbindungen / Eigenschaften von Internetprotokoll (TCP/IP)).



Authentisierung

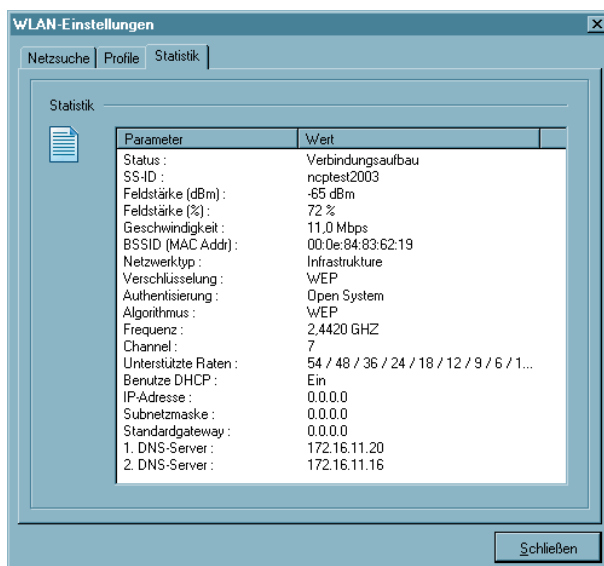
In diesem Fenster können die Zugangsdaten für eine automatische Anmeldung am HotSpot eingetragen werden. Diese Benutzerdaten werden nur für dieses WLAN-Profil verwendet.

Die Authentisierung kann durch Eintragen von Benutzername und Passwort in die Eingabemaske des HotSpot-Betreibers erfolgen oder über Script. Das Script automatisiert die Anmeldung beim HotSpot-Betreiber.



Beachten Sie dabei, dass die Verbindung über einen HotSpot-Betreiber gebührenpflichtig ist. Sie müssen den Geschäftsbedingungen des HotSpotbetreibers zustimmen, wenn die Verbindung aufgebaut werden soll.

Statistik



Das Statistik-Fenster der WLAN-Einstellungen zeigt im Klartext den Status der Verbindung zum Access Point.

Die Statistik ergänzt die grafische Anzeige im Monitor, worin die Feldstärke des Funknetzes angezeigt wird, um zusätzliche Daten.

4.2.4 Amtsholung



Eine Amtsholung ist dann nötig, wenn der IPSec Client an einer Nebenstellenanlage betrieben wird. Damit die definierten Profile des IPSec Clients auch im mobilen Einsatz verwendbar bleiben, ohne Rufnummern umkonfigurieren zu müssen, kann, sofern an einem Anschluss eine Amtsholung nötig wird, diese hier eingetragen werden. Die Nummer für die Amtsholung wird dann für alle Zielrufnummern der Profile automatisch mitgewählt.

Bei der Eingabe der Amtsholung sind als Eingabezeichen die Zahlen 0-9 und die Zeichen '#' und '*' möglich.

Wird ein Komma "," eingegeben, so wird über die Amtsholung eine Wählpause konfiguriert.

4.2.5 Zertifikate |Konfiguration



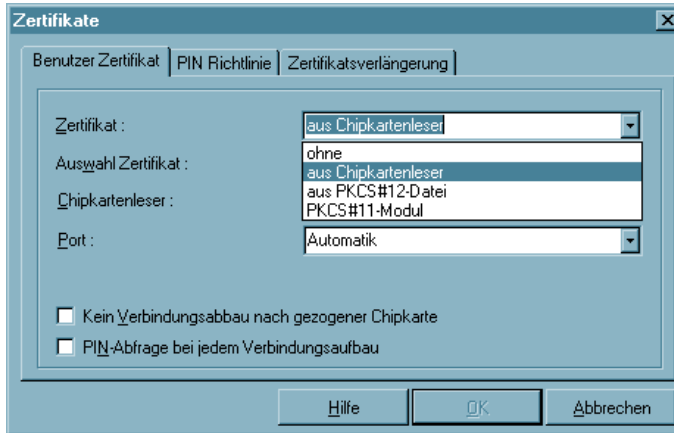
Unter diesem Menüpunkt wird konfiguriert welche Art von Zertifikaten eingesetzt werden – ob Soft-Zertifikate oder Zertifikate auf Chipkarten (Smart Cards) – und wo diese Zertifikate auf dem Rechnersystem zu finden sind. Deweiteren wird die Dauer der Gültigkeit eines Zertifikats festgelegt und können die Richtlinien für die PIN definiert werden.

Zertifikate (Certificates) werden von einer CA (Certification Authority) mittels PKI-Manager (Software) ausgestellt. Sie können als Soft-Zertifikat in Dateiform ausgeliefert werden oder auf eine Smart Card (Chipkarte) gebrannt werden. Diese Smart Card enthält u.a. mit den Zertifikaten digitale Signaturen, die ihr den Status eines digitalen Personalausweises verleihen. Es können Zertifikate eingesetzt werden, die einen privaten Schlüssel bis zu einer Länge von 2048 Bits haben. Als Gegenstelle muss der NCP Secure Server 5.21 oder höher eingesetzt werden.

Die Client Software überwacht, ob eine PKCS#12-Datei vorhanden ist. Wird eine PKCS#12-Datei (Soft-Zertifikat) eingesetzt, z.B. auf einem USB-Stick oder einer SD-Karte gespeichert, so wird nach dem Ziehen der SD-Karte die PIN zurückgesetzt und eine bestehende Verbindung abgebaut. Dieser Vorgang entspricht dem “Verbindungsabbau bei gezogener Chipkarte”, der bei Verwendung einer Chipkarte im Monitormenü unter “Konfiguration / Benutzer-Zertifikat” eingestellt werden kann. Wird später die SD-Karte wieder gesteckt, kann nach der erneuten PIN-Eingabe die Verbindung wieder hergestellt werden.

In der Zertifikats-Konfiguration können für die Pfad-Angaben die Umgebungsvariablen (Benutzer) des Betriebssystems eingesetzt werden. Die Variablen werden beim Schießen des Dialogs und beim Einlesen des Telefonbuches umgewandelt und in die Konfiguration zurück geschrieben. Existiert eine Umgebungsvariable nicht, wird sie aus dem Pfad beim Umwandeln entfernt und ein Log-Eintrag ins Logbuch geschrieben. Fehlt ein %-Zeichen (Syntax), bleibt die Variable stehen und es wird ebenfalls ein Log-Eintrag geschrieben.

■ Benutzer-Zertifikat



Zertifikat

Klicken Sie auf die Menüabzweigung “Konfiguration – Zertifikate”, so können Sie zunächst bestimmen, ob Sie die Zertifikate und damit die “Erweiterte Authentisierung” nutzen wollen, und wo Sie die Benutzer-Zertifikate hinterlegen wollen.

In weiteren Konfigurationsfeldern werden die Richtlinien zur PIN-Eingabe festgelegt und das Zeitintervall eingestellt innerhalb dessen das Zertifikat abläuft bzw. eine Zertifikatsverlängerung beantragt werden muss.

- ohne:** Wählen Sie in der Listbox “Zertifikat” die Einstellung “ohne”, so wird kein Zertifikat ausgewertet und die “Erweiterte Authentisierung” findet nicht statt.
- aus Chipkartenleser:** Wählen Sie “aus Chipkartenleser” in der Listbox, so werden bei der “Erweiterten Authentisierung” die relevanten Zertifikate von der Smart Card in ihrem Chipkartenleser ausgelesen.
- aus PKCS#12-Datei:** Wählen Sie “aus PKCS#12-Datei” aus der Listbox, so werden bei der “Erweiterten Authentisierung” die relevanten Zertifikate aus einer Datei auf der Festplatte Ihres Rechners gelesen.
- PKCS#11-Modul:** Wählen Sie “PKCS#11-Modul” in der Listbox, so werden bei der “Erweiterten Authentisierung” die relevanten Zertifikate von der Smart Card in einem Chipkartenleser oder von einem Token gelesen.

Chipkartenleser

Wenn Sie die Zertifikate von der Smart Card mit Ihrem Lesegerät nutzen wollen, wählen Sie Ihren Chipkartenleser aus der Listbox. (Siehe auch → PIN eingeben)

Chipkartenleser (PC/SC-konform)

Die Client Software unterstützt automatisch alle Chipkartenleser, die PC/SC-konform sind. Die Client Software erkennt dann den Chipkartenleser nach einem Boot-Vorgang automatisch. Erst dann kann der installierte Leser ausgewählt und genutzt werden.

Die PC/SC-Schnittstelle wird nur geöffnet, wenn ein Verbindungsaufbau stattfindet, bei dem ein Chipkartenzugriff erfolgt. D.h. auch andere Applikationen können im “exclusiven” Modus die PC/SC-Schnittstelle öffnen.

Chipkartenleser (CT-API-konform)

Mit der aktuellen Software werden Treiber für die Modelle SCM Swapsmart und SCM 1x0 (PIN Pad Reader) mitgeliefert. Sollte der Chipkartenleser mit den mitgelieferten Treibern nicht funktionieren oder ein anderer Chipkartenleser installiert sein, wenden Sie sich unbedingt an den Hersteller. Nehmen Sie außerdem folgende Einstellung in der Client Software vor: Editieren Sie die Datei NCPPKI.CONF, befindlich im Installationsverzeichnis, indem Sie als “ReaderName” den Namen des angeschlossenen Chipkartenlesers (xyz) eintragen und als DLLWIN95 bzw. DLLWINNT den Namen des installierten Treibers eintragen. Für die NT-basierenden Betriebssysteme Windows 2000 und Windows XP ist der Modulname DLLWINNT zu benutzen. (Der Standardname für CT-API-konforme Treiber ist CT32.DLL).

Wichtig: Nur die Treiber sind in der Liste sichtbar, die mit “visible = 1” auf sichtbar gesetzt wurden!

```
ReaderName = SCM Swapsmart (CT-API) -> xyz
DLLWIN95   = scm20098.dll           -> ct32.dll
DLLWINNT   = scm200nt.dll           -> ct32.dll
```



Nach einem Boot-Vorgang erscheint der “ReaderName” im Monitor-Menü an dieser Stelle, wenn in der Datei NCPPKI.CONF für den Treiber “visible = 1” gesetzt wurde!

Port

Der Port wird bei korrekter Installation des Lesegeräts automatisch bestimmt. Bei Unstimmigkeiten können die COM Ports 1-4 gezielt angesteuert werden.

Auswahl Zertifikat

1. Zertifikat ... 3.: (Standard = 1) Aus der Listbox kann aus bis zu drei verschiedenen Zertifikaten gewählt werden, die sich auf der Chipkarte befinden. Die Anzahl der Zertifikate auf der Chipkarte ist abhängig von der Registration Authority, die diese Karte brennt. Wenden Sie sich zu weiteren Fragen bitte an Ihren Systemadministrator.

Auf den Chipkarten von Signtrust und NetKey 2000 befinden sich drei Zertifikate:

- (1) zum Siginieren
- (2) zum Ver- und Entschlüsseln
- (3) zum Authentisieren (optional bei NetKey 2000)

PKCS#12-Dateiname

Nutzen Sie das PKCS#12-Format, so erhalten Sie von Ihrem Systemadministrator eine Datei, die auf der Festplatte Ihres Rechners eingespielt werden muss. In diesem Fall muss Pfad und Dateiname der PKCS#12-Datei eingegeben, bzw. nach einem Klick auf den [...] -Button (Auswahl-Button) die Datei ausgewählt werden.

PKCS#11-Modul

Nutzen Sie das PKCS#11-Format, so erhalten Sie eine DLL vom Hersteller des Chipkartenlesers oder des Tokens, die auf der Festplatte Ihres Rechners eingespielt werden muss. In diesem Fall muss Pfad und Dateiname des Treibers eingegeben werden.



Editieren Sie die Datei NCPPKI.CONF, befindlich im Installationsverzeichnis, indem Sie als "Modulname" den Namen des angeschlossenen Lesers oder Tokens (xyz) eintragen. Als PKCS#11-DLL muss der Name der DLL eingegeben werden. Der zugehörige "Slotindex" ist herstellerabhängig (Standard = 0).

Modulname = xyz
 PKCS#11-DLL = Name der DLL
 Slotindex =

Nach einem Boot-Vorgang erscheint der von Ihnen eingetragene "Modulname" im Monitormenü an dieser Stelle, wenn in der Datei NCPPKI.CONF für den Treiber "visible = 1" gesetzt wurde!



Sie können auch mit Hilfe eines Assistenten nach installierten PKCS#11-Modulen suchen und das gewünschte Modul mit dem dazugehörigen Slot selektieren. Dazu klicken Sie auf den Button in der Zeile mit "PKCS'11-Modul."

Kein Verbindungsabbau bei gezogener Chipkarte

Beim Ziehen der Chipkarte wird nicht unbedingt die Verbindung abgebaut. Damit "Kein Verbindungsabbau bei gezogener Chipkarte" erfolgt, muss diese Funktion aktiviert werden.

PIN-Abfrage bei jedem Verbindungsaufbau

Standardeinstellung: Wird diese Funktion nicht genutzt, so wird die PIN nur einmalig beim ersten Verbindungsaufbau des IPSec Clients abgefragt.

Wird diese Funktion aktiviert, so wird bei jedem Verbindungsaufbau die PIN erneut abgefragt.



Wichtig: Ist der Monitor nicht gestartet, kann kein PIN-Dialog erfolgen. In diesem Fall wird bei einem automatischen Verbindungsaufbau die Verbindung ohne erneute PIN-Eingabe hergestellt!

■ PIN-Richtlinie

Zertifikate

Benutzer Zertifikat | **PIN Richtlinie** | Zertifikatsverlängerung

Minimale Anzahl der Zeichen:

☐ PIN darf nur Zahlen enthalten

☒ PIN muss ein Sonderzeichen enthalten

☒ PIN muss einen Großbuchstaben enthalten

☐ PIN muss einen Kleinbuchstaben enthalten

☐ PIN muss eine Zahl enthalten

☐ PIN darf kein Zeichen öfter als die Hälfte der PIN-Länge wiederholen

Hilfe OK Abbrechen

Für die PIN können Richtlinien festgelegt werden, die bei Eingabe oder Änderung der PIN beachtet werden müssen.

Minimale Anzahl der Zeichen

Standard ist eine 6-stellige PIN. Aus Sicherheitsgründen werden 8 Stellen empfohlen.

Weitere Richtlinien

Es wird empfohlen alle PIN-Richtlinien einzusetzen, außer der, dass nur Zahlen enthalten sein dürfen. Zudem sollte die PIN nicht mit einer Zahl beginnen. Die vorgegebenen Richtlinien werden eingeblendet, wenn die PIN geändert wird und die Richtlinien, die bei der Eingabe erfüllt werden, werden grün markiert (siehe → PIN ändern).

■ Zertifikatsverlängerung

Zertifikate

Benutzer Zertifikat | PIN Richtlinie | **Zertifikatsverlängerung**

☒ Warnung vor Zertifikatsablauf aktivieren

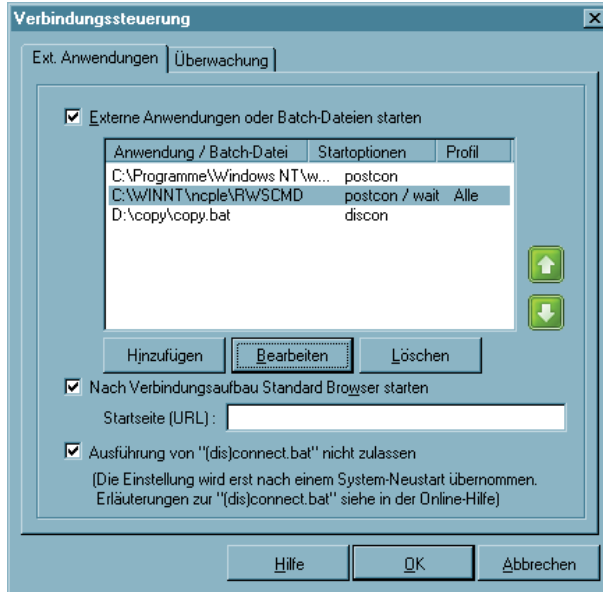
Tage vor Zertifikatsablauf Warnung anzeigen

Hilfe OK Abbrechen

In diesem Konfigurationsfeld kann eingestellt werden, ob und wie viele Tage vor Ablauf der Gültigkeit des Zertifikats eine Meldung ausgegeben werden soll, die vor dem Ablauf der Gültigkeit warnt. Sobald die eingestellte Zeitspanne vor Ablauf in Kraft tritt, wird bei jeder Zertifikatsverwendung eine Meldung aufgeblendet, die auf das Ablaufdatum des Zertifikats hinweist.

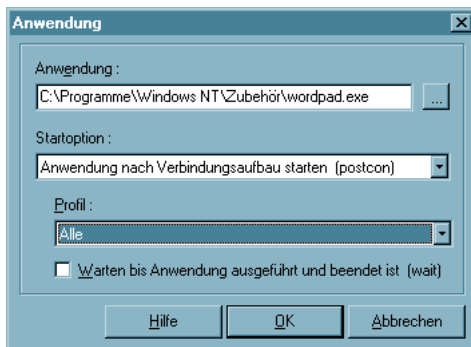
4.2.6 Verbindungssteuerung | Konfiguration

■ Externe Anwendungen



Über dieses Konfigurationsfeld können in Abhängigkeit vom Client Monitor Anwendungen oder Batch-Dateien gestartet werden. Die externen Anwendungen werden wie unten beschrieben eingefügt. Die Reihenfolge ihres Aufrufs von oben nach unten kann mit den grünen Pfeiltasten verändert werden.

Wollen Sie nach dem Verbindungsaufbau den Standard-Browser starten, so aktivieren Sie diese Funktion und tragen die Website des Browsers ein.



Nachdem Sie die Funktion “Externe Anwendungen oder Batch-Dateien starten” selektiert haben, können Sie über den Button mit “Hinzufügen” eine Anwendung oder Batch-Datei vom Rechner selektieren, die je nach Startoption geladen wird:

- vor Verbindungsaufbau starten (precon)
- nach Verbindungsaufbau starten (postcon)
- nach Verbindungsabbau starten (discon)

Zusätzlich können diese auszuführenden Anwendungen auch an ein bestimmtes Profil gebunden werden.

Die Wait-Funktion “Warten bis Anwendung ausgeführt und beendet ist” kann dann von Bedeutung sein, wenn eine Reihe von Batch-Dateien nacheinander ausgeführt werden soll.

Ausführung von “(dis)connect.bat” nicht zulassen



Diese Funktion sollte immer aktiviert sein, wenn nicht unbedingt für eine gewünschte Anwendung die Ausführung der genannten Batch-Dateien mit Administrator-(System-) Rechten erforderlich ist. (Beachten Sie dazu die Beschreibung im Handbucheintrag “Services”). Die Anwendungen (Batch-Dateien) für deren Ausführung Benutzerrechte genügen, können oben im Monitormenü “Externe Anwendungen starten” eingetragen werden (siehe oben).

■ Überwachung

The screenshot shows the 'Verbindungssteuerung' dialog box with the 'Überwachung' tab selected. The settings are as follows:

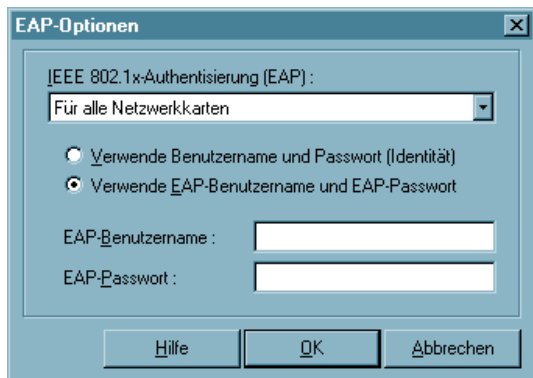
- ☒ Aktiviere Verbindungssteuerung
- ☒ automatischer Verbindungsabbau bei Überschreitung
- ☒ Meldung bei Überschreitung
- ☐ Vorwarnung bei 90% der Maximalwerte
- Zeitraum der Überwachung: 5 Tage 0 Std 0 Min
- ☒ Überwachen des Zeitlimits
- maximale Verbindungszeit: 0 Tage 2 Std 0 Min
- ☐ Überwachen der maximalen Verbindungsaufbauten
- max. Anzahl der Verbindungen: 0
- ☐ Überwachen der maximalen Gebühreneinheiten
- max. Anzahl der Einheiten: 0

Buttons at the bottom: Hilfe, OK, Abbrechen.

Die “Verbindungssteuerung” kann eine automatische Überwachung bewirken. So können Sie wählen, welche der Limits Sie sich für Ihre Kommunikation setzen (Überwachen des Zeitlimits, der maximalen Verbindungsaufbauten und/oder der maximalen Gebühreneinheiten), für welchen Zeitraum diese Limits gültig sein sollen (Zeitraum der Überwachung) und wie Sie von Limit-Überschreitungen in Kenntnis gesetzt werden möchten (Meldung und Vorwarnung), oder ob ein automatischer Verbindungsabbau stattfinden soll.

Wenn ein von Ihnen definiertes Limit überschritten wurde, wird jede weitere Kommunikation unterbunden, bis Sie die “Sperre” wieder aufgehoben haben (siehe → Verbindung, Sperre aufheben).

4.2.7 EAP-Optionen



In den “EAP-Optionen” kann angegeben werden, ob die EAP-Authentisierung nur über WLAN-, LAN- oder alle Netzwerkkarten erfolgen soll. Die hier gemachte Einstellung gilt global für alle Einträge des Telefonbuchs. In der Aktivierungsbox kann die EAP-Authentisierung wie folgt eingestellt werden:

- Deaktiviert
- Für alle Netzwerkkarten
- Nur für WLAN-Karten
- Nur für LAN-Karten

Das Extensible Authentication Protocol Message Digest5 (EAP MP5) kann dann zum Einsatz kommen, wenn für den Zugang zum LAN ein Switch oder für das wireless LAN ein Access Point verwendet werden, die 802.1x-fähig sind und eine entsprechende Authentisierung unterstützen.

Mit dem Extensible Authentication Protocol (EAP MP5) kann verhindert werden, dass sich unberechtigte Benutzer über die Hardware-Schnittstelle in das LAN einklinken.

Zur Authentisierung kann wahlweise “VPN-Benutzername” mit “VPN-Passwort” (aus dem Konfigurationsfeld “Identität”) verwendet werden oder ein eigener “EAP-Benutzername” mit einem “EAP-Passwort”.



Zertifikatsinhalte können dergestalt automatisch übernommen werden, indem im Telefonbuch unter “Tunnel-Parameter” VPN-Benutzername und VPN-Passwort vom Zertifikat übernommen werden und in den EAP-Optionen “Verwende VPN-Benutzername und VPN-Passwort” aktiviert wird.

Bei EAP-TLS (mit Zertifikat) kann der EAP-Benutzername direkt aus der Zertifikats-Konfiguration bezogen werden. Folgende Inhalte des konfigurierten Zertifikats können genutzt werden, indem in die EAP-Konfiguration die entsprechenden Platzhalter eingegeben werden:

```
Commonname : %CERT_CN%
E-Mail      : %CERT_EMAIL%
```



Nach Konfiguration des EAP erscheint eine Statusanzeige im grafischen Feld des Monitors. Durch einen Doppelklick auf das EAP-Symbol kann das EAP zurückgesetzt werden. Anschließend erfolgt automatisch eine erneute EAP-Verhandlung.

4.2.8 Logon Optionen



Die Logon-Optionen werden erst dann wirksam, wenn der Rechner gebootet wird.

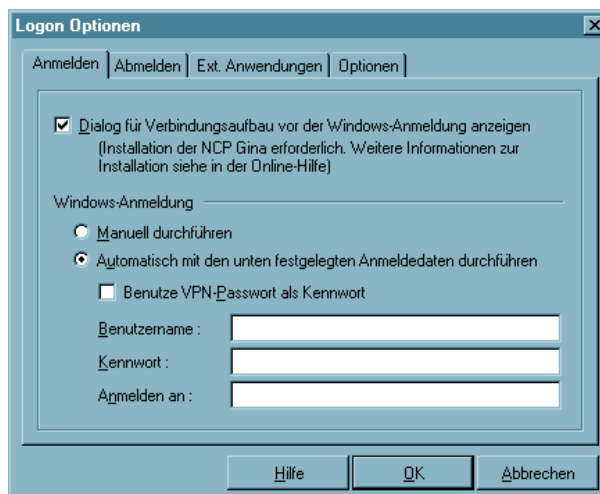
■ Anmelden

Da der Verbindungsaufbau zum Gateway vor dem Windows Logon stattfindet, erfolgt die Anmeldung an der remote Domain bereits verschlüsselt und mit aktivierter Firewall.

Dialog für Verbindungsaufbau vor Windows-Anmeldung anzeigen



Die Dialoge der NCP Gina können hier ausgeblendet werden, ohne dass dabei die Gina deinstalliert wird. Für die jeweilige Arbeitsumgebung eventuell nötige Gina-Verkettungen bleiben auf diese Weise bestehen. Soll der Gina-Dialog eingeblendet werden, so ist darauf zu achten, dass die NCP Gina auf jeden Fall installiert sein muss. Dies kann auf dreierlei Weise stattfinden:



– Bei der Software-Installation; hierbei wird der Benutzer gefragt, ob er die Windows-Anmeldung über die NCP Gina nutzen will. Wenn ja, wird sie installiert.

– Eine nachträgliche Installation ist über die Kommandozeilen-Schnittstelle `rwscmd.exe` möglich, ebenso die nachträgliche Deinstallation. (Siehe dazu den Anhang “Services”).

– Die Gina wird auch installiert, wenn über das Enterprise Management ein entsprechendes Telefonbuch bereitgestellt wird.

Sie müssen den “Dialog für Verbindungsaufbau vor Windows-Anmeldung anzeigen” lassen, damit bereits in der Boot-Phase die Verbindung zum VPN Gateway hergestellt werden kann. Für diesen Verbindungsaufbau müssen ggf. die Zugangsdaten für die Netzeinwahl bzw. PIN und SIM-PIN vor der Windows-Anmeldung eingegeben werden.

Windows-Anmeldung

Die nachfolgende Windows-Anmeldung kann je nach Konfiguration manuell durchgeführt werden oder automatisch.

“Manuell durchführen” bedeutet, dass der Benutzer seine Anmeldedaten per Hand in die Windows-Anmeldemaske eingibt.

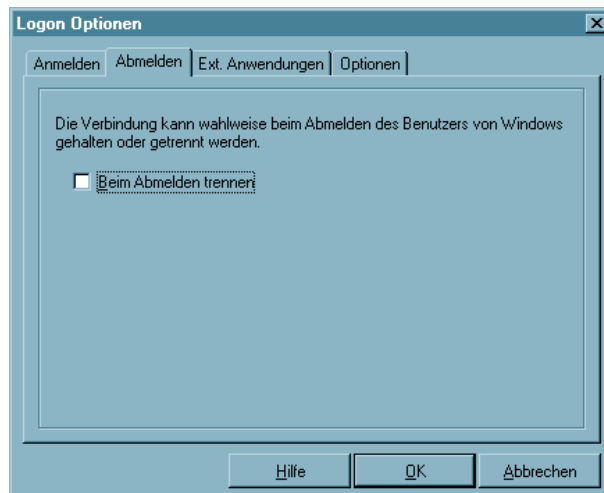
“Automatisch” bedeutet, dass die Client Software die hier eingetragenen Daten ohne Zutun des Benutzers an die Microsoft Gina übergibt.



Wenn Sie die Logon-Option mit Rückruf nutzen, muss “Verhandle PPP Callback” aktiviert werden (siehe → Parameterfeld “Rückruf” im Telefonbuch).

Zur Anwahl an das Zielsystem mit der Logon-Option beachten Sie bitte den Abschnitt “Eine Verbindung herstellen – Client Logon” und den Anhang zum Mobile Computing.

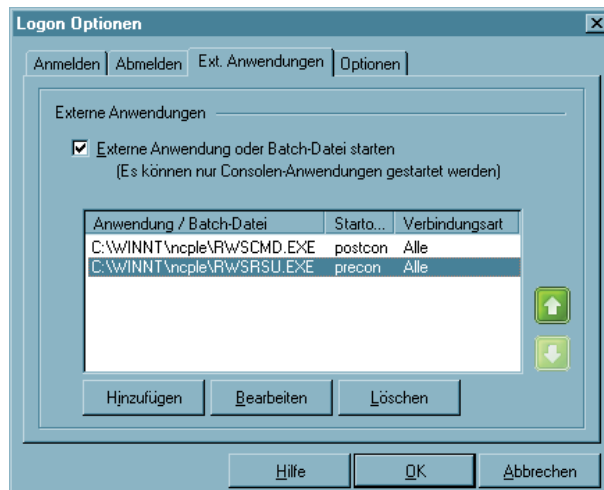
■ Abmelden



Die Verbindung des Clients zum VPN Gateway oder ISP kann beibehalten werden, wenn eine Windows-Abmeldung erfolgt.

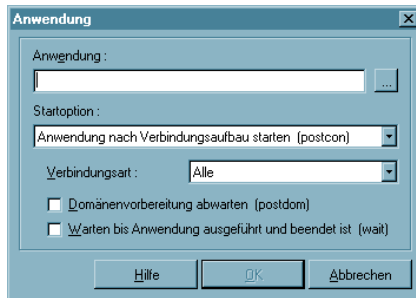
Dies gestattet einen Windows-Benutzerwechsel am Rechner vornehmen zu können, ohne die VPN-Verbindung abbauen zu müssen.

■ Externe Anwendungen



Über dieses Konfigurationsfeld können in Abhängigkeit vom Client Monitor Consolen-Anwendungen oder Batch-Dateien gestartet werden (keine Windows-Programme!).

Die externen Anwendungen werden wie auf der nächsten Seite beschrieben eingefügt. Die Reihenfolge ihres Aufrufs von oben nach unten kann mit den grünen Pfeiltasten verändert werden.



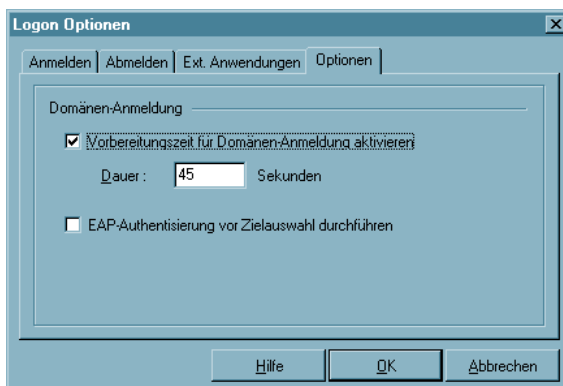
Nachdem Sie die Funktion “Externe Anwendungen oder Batch-Dateien starten” selektiert haben, können Sie über den Button mit “Hinzufügen” (siehe vorige Seite) eine Anwendung oder Batch-Datei vom Rechner selektieren, die je nach Startoption geladen wird:

- vor Verbindungsaufbau starten (precon)
- nach Verbindungsaufbau starten (postcon)

Die Anwendung kann außerdem in Abhängigkeit von der Verbindungsart des im Gina-Dialog selektierten Zielsystems gestartet werden. Die Applikation wird immer gestartet, wenn als Verbindungsart “Alle” gewählt wurde.

“Domänenvorbereitung abwarten (postdom)” bedeutet, dass die Anwendung nach der Initialisierungszeit unmittelbar vor der Domänenanmeldung gestartet wird. Die Wait-Funktion “Warten bis Anwendung ausgeführt und beendet ist” kann dann von Bedeutung sein, wenn eine Reihe von Batch-Dateien nacheinander ausgeführt werden soll.

■ Optionen



Zwischen Netzanmeldung und Domänen-Anmeldung kann Windows eine gewisse Initialisierungszeit benötigen. Diese Vorbereitungszeit für die Domänenanmeldung kann hier aktiviert und eingestellt werden. Die Windows-Anmeldung findet erst nach der hier eingestellten Initialisierungszeit nach dem Verbindungsaufbau statt. Der Standardwert beträgt 45 Sekunden und kann nach Bedarf verändert werden.

EAP-Authentisierung vor Zielauswahl durchführen

Standardmäßig erfolgt die EAP-Authentisierung vor dem Verbindungsaufbau zum VPN Gateway. Soll EAP genutzt werden, ohne dass anschließend eine Verbindung über den Client (reiner EAP Client) aufgebaut werden soll, so muss diese Funktion aktiviert werden. Wird EAP mit Zertifikat eingesetzt, so erscheint der PIN-Dialog zur Authentisierung an den Netzwerkkomponenten. Danach kann die Zielauswahl erfolgen. Wird die Funktion nicht aktiviert, findet die EAP-Authentisierung erst nach der Zielauswahl statt.



Beachten Sie zu den Logon-Optionen auch die Beschreibung “Domänenanmeldung mit der NCP Gina” im Anhang “Mobile Computing via GPRS/UMTS”

4.2.9 Konfigurations-Sperren

Über die Konfigurations-Sperren kann das Konfigurations-Hauptmenü im Monitor so modifiziert werden, dass der Benutzer die voreingestellten Konfigurationen nicht mehr abändern kann, bzw. ausgewählte Parameterfelder für den Benutzer nicht sichtbar sind.



Die Konfigurations-Sperren werden in der definierten Form erst wirksam, wenn die Einstellungen mit "OK" übernommen werden. Wird der "Abbrechen"-Button gedrückt, wird auf die Standard-Einstellung zurückgesetzt.

■ Allgemein | Konfigurations-Sperren

Konfigurations - Sperren

Allgemein | Profile

ID für Konfigurations-Sperre

Benutzer:

Passwort:

Bestätigung Passwort:

Konfigurations-Berechtigungen

- ☒ Erweiterte Firewall-Einstellungen
- ☒ Zertifikate
- ☒ Verbindungssteuerung
- ☒ EAP-Optionen
- ☒ Logon-Optionen

Hilfe Ok Abbrechen

Um die Konfigurations-Sperren wirksam festlegen zu können, muss eine ID eingegeben werden, die sich aus "Benutzer" und "Passwort" zusammensetzt. Das Passwort muss anschließend bestätigt werden.

Bitte beachten Sie, dass die ID für die Konfigurations-Sperre unbedingt nötig ist, die Sperren wirksam werden zu lassen oder die Konfigurations-Sperren auch wieder aufzuheben. Wird die ID vergessen, besteht keine Möglichkeit mehr, die Sperren wieder aufzuheben!

Anschließend kann die Berechtigung, die Menüpunkte unter dem Hauptmenüpunkt "Konfiguration" zu öffnen, für den Benutzer eingeschränkt werden. Standardmäßig kann der Benutzer alle Menüpunkte öffnen und die Konfigurationen bearbeiten. Wird zu einem Menüpunkt der zugehörige Haken mit einem Mausklick entfernt, so kann der Benutzer diesen Menüpunkt nicht mehr öffnen.

■ Profile | Konfigurations-Sperren

Die Bearbeitungsrechte für die Parameter in den Profil-Einstellungen sind in zwei Sparten unterteilt:

- Allgemeine Rechte
- Sichtbare Parameterfelder der Profile



Allgemeine Rechte

Die allgemeinen Rechte beziehen sich nur auf die (Konfiguration der) Profile. Wird festgelegt "Profile dürfen neu angelegt werden", "Profile dürfen konfiguriert werden" bleibt jedoch ausgeschlossen, so können zwar mit dem Assistenten neue Profile definiert werden, eine nachfolgende Änderung einzelner Parameter ist dann jedoch nicht mehr möglich.

Sichtbare Parameterfelder der Profile

Die Parameterfelder der Profil-Einstellungen können für den Benutzer ausgeblendet werden.



Beachten Sie, dass Parameter eines nicht sichtbaren Feldes auch nicht konfiguriert werden können.

4.2.10 Profile importieren

Über diese Funktion können Profil-Einstellungen vom Client eingelesen werden. Diese Profil-Einstellungen können in Form einer INI-Datei vom Zielsystem erstellt oder manuell editiert werden. Im Installationsverzeichnis befinden sich dazu die Beispieldateien IMPORT_D.TXT und IMPORT_E.TXT. In den Beispieldateien sind auch Syntax und Parameterwerte beschrieben.

4.2.11 HotSpot



Unter diesem Menüpunkt erfolgt die Konfiguration zur HotSpot-Anmeldung. Folgende Einstellungen sind möglich:

– “Standard-Browser für HotSpot-Anmeldung verwenden” ist die Standardeinstellung. Wird der Haken in der Checkbox entfernt, kann ein anderer Browser angegeben werden in der Form:

`%PROGDIR%\Mozilla\Firefox\firefox.exe.`

Der alternative Browser kann speziell für die Anforderungen am HotSpot konfiguriert werden. D. h. es wird kein Proxy Server konfiguriert und alle aktiven Elemente (Java, Javascript, ActiveX) werden deaktiviert. (Der alternative Browser ist nicht Bestandteil der Client Software!) Darüber hinaus kann der MD5-Hash-Wert der Browser-Exe-Datei ermittelt und in das Feld “MD5-Hash” eingetragen werden. Auf diese Weise wird sichergestellt, dass nur mit diesem Browser eine HotSpot-Verbindung zustande kommt.

– Unter “Startseite / Adresse” wird die oben beschriebene Startseite eingegeben in der Form:

`http://www.mycompagnie.de/error.html.`

4.2.12 Profil-Sicherung

Existiert noch kein gesichertes Profil, zum Beispiel bei einer Erstinstallation, so wird automatisch ein erstes angelegt (NCPPHONE.SAV).

■ Erstellen

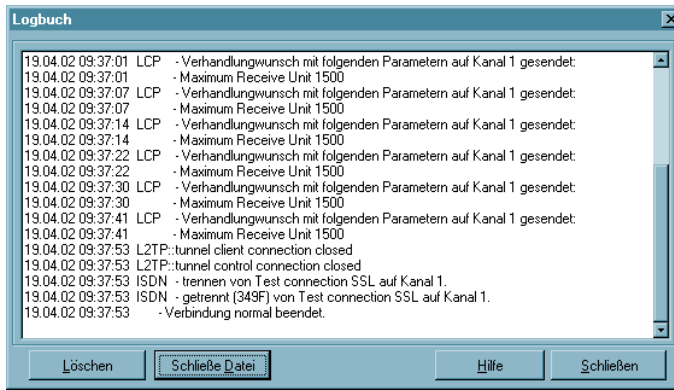
Nach jedem Klick auf den Menüpunkt “Erstellen” wird nach einer Sicherheitsabfrage eine Profil-Sicherung angelegt, die die Konfiguration zu diesem Zeitpunkt enthält.

■ Wiederherstellen

Nach jedem Klick auf “Wiederherstellen” wird die letzte Profil-Sicherung eingelesen. Änderungen in der Konfiguration, die seit der letzten Profil-Sicherung vorgenommen wurden gehen damit verloren.

4.3 Log

Mit der Log-Funktion werden die Kommunikationsereignisse der IPSec Client Software mitprotokolliert. Wählen Sie die Log-Funktion an, öffnet sich das Fenster des "Logbuches".



Die hier abgebildeten Daten werden bis zum nächsten Reboot im Speicher gehalten.

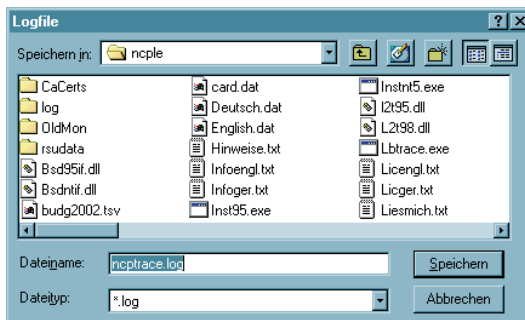
Eine zusätzliche Log-Datei speichert die Aktionen des Clients selbständig für die letzten sieben Tage. Log-Ausgaben, die älter als sieben Betriebstage sind, werden automatisch gelöscht. Die Datei steht im Installations-Verzeichnis unter LOG\ und heißt NCPyymmdd.LOG. Sie wird mit Datumsangabe (yymmdd) immer bei Beenden des Monitors geschrieben. Die Datei kann mit einem Texteditor geöffnet und analysiert werden.

■ Logbuch

Die Buttons des Logbuchfensters haben folgende Funktionen:

- Öffne Datei
- Schließe Datei
- Löschen – Fensterinhalt
- Schließen – Log-Fenster

Öffne Datei



Wenn Sie auf diesen Button klicken, erhalten Sie in einem weiteren Fenster die Möglichkeit Name und Pfad einer Datei einzugeben, in die der Inhalt des Log-Fensters geschrieben wird (Standard: ncptrace.log).

Alle Transaktionen mit der IPSec Client Software, wie Anwahl und Empfang, einschließlich der Rufnummern, werden automatisch mitprotokolliert und in diese Datei geschrieben, bis Sie auf den Button mit “Schließe Datei” klicken. Wenn Sie eine Log-Datei anlegen, können Sie die Transaktionen mit dem IPSec Client über einen längeren Zeitraum verfolgen.

Schließe Datei

Wenn Sie auf diesen Button klicken, wird die Datei geschlossen, die Sie mit “Öffne Datei” angelegt haben. Die geschlossene Log-Datei kann zur Analyse der Transaktionen mit dem IPSec Client oder zur Fehlersuche verwendet werden.

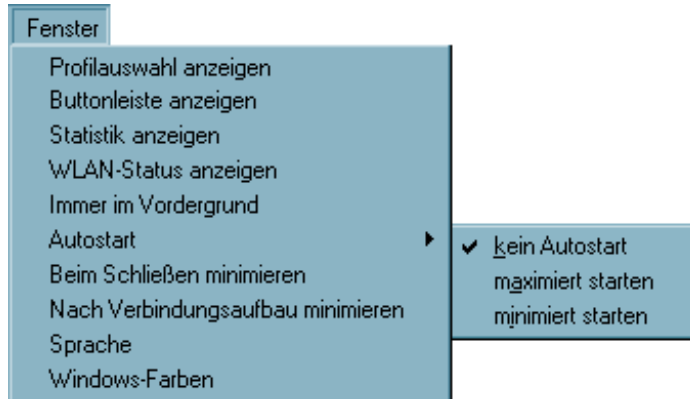
Löschen – Fensterinhalt

Wenn Sie auf diesen Button drücken wird der Inhalt des Log-Fensters gelöscht.

Schließen – Log-Fenster

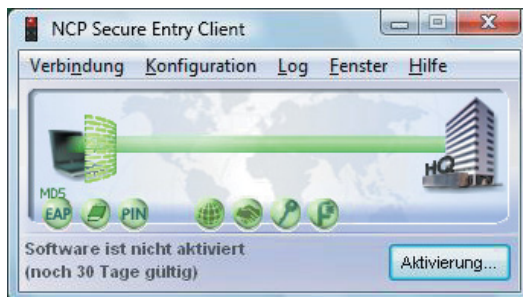
Wenn Sie auf “Schließen” klicken, schließen Sie das Fenster des “Logbuches” und kehren zum Monitor zurück.

4.4 Fenster



Unter dem Menüpunkt “Fenster” können Sie die Bedienoberfläche des Monitors variieren und die Sprache für die Monitoroberfläche festlegen.

4.4.1 Profilauswahl anzeigen



Links: Minimierte Darstellung



Wenn Sie auf “Profilauswahl anzeigen” klicken, kann aus der Liste der konfigurierten Profile das gewünschte ausgewählt werden (Bild unten).

4.4.2 Buttonleiste anzeigen



Wenn Sie auf “Buttonleiste anzeigen” klicken, werden Buttons für die Menüpunkte “Verbinden” und “Trennen” aus dem Hauptmenü “Verbindung” eingeblendet.

4.4.3 Statistik anzeigen



Wenn Sie auf “Statistik anzeigen” klicken, werden Informationen zu Datenmenge, Verbindungszeit, Timeout etc. angezeigt. Die Monitor-Oberfläche ist dann entsprechend größer.

4.4.4 WLAN-Status anzeigen

Unabhängig vom Verbindungsmedium des aktuell selektierten Linkprofils kann das Feld zur grafischen Anzeige des WLAN-Status geöffnet bzw. geschlossen werden, wenn im Monitormenü “Konfiguration” unter “WLAN-Einstellungen” eine WLAN-Konfiguration aktiviert wurde. Wurde eine Multifunktionskarte konfiguriert, ist der Menüpunkt “WLAN-Status anzeigen” nicht aktiv.

4.4.5 Immer im Vordergrund

Wenn Sie “Immer im Vordergrund” geklickt haben, wird der Monitor immer im Bildschirmvordergrund angezeigt, unabhängig von der jeweils aktiven Anwendung.

4.4.6 Autostart

Mit diesem Menüpunkt wird der Monitor so eingestellt, dass er nach dem Booten selbstständig startet. “Autostart” ersetzt den Menüpunkt “Fenster – Nach Booten starten”. Über den neuen Menüpunkt können folgende Optionen eingestellt werden:

- ☐ kein Autostart: nach dem Booten nicht automatisch starten
- ☐ minimiert starten: nach dem Booten den Monitor starten und minimiert darstellen
- ☐ maximiert starten: nach dem Booten den Monitor starten und in normaler Größe darstellen



Wenn Sie oft mit der IPSec Client Software arbeiten und die Informationen des Monitors benötigen, so sollten Sie die Einstellung “maximiert starten” wählen. Prinzipiell ist es für die Kommunikation mit dem Zielsystem nicht nötig, den Monitor zu starten.

4.4.7 Beim Schließen minimieren

Wird der Monitor bei einer bestehenden Verbindung über den Schließen-Button [x] rechts in der Kopfzeile oder das Systemmenü links in der Kopfzeile geschlossen [Alt + F4], so informiert ein Meldungsfenster darüber, dass kein Ampelsymbol (Tray Icon) mehr in der Task-Leiste erscheint, worüber der Status dieser Verbindung kontrolliert werden könnte, d.h. der Benutzer kann dann auf der Oberfläche seines Desktops nicht erkennen, ob und wie lange noch Verbindungsgebühren anfallen, oder ob die Verbindung bereits beendet wurde.

(Um in diesem Fall den Status der Verbindung zu erfahren und sie gegebenenfalls korrekt zu beenden, muss der Monitor erneut gestartet werden.)

Ist dieser Menüpunkt aktiviert, so wird der Monitor beim Schließen über den Button [x] rechts in der Kopfzeile oder über [Alt + F4] nur minimiert und erscheint als Ampelsymbol in der Task-Leiste, worüber der Status der Verbindung abgelesen werden kann. Der Klick auf den Schließen-Button [x] der Kopfzeile hat in dieser Einstellung die gleiche Wirkung wie der Klick auf den Minimieren-Button [-] der Kopfzeile.

(In der Darstellung des Ampelsymbols in der Task-Leiste kann nach einem rechten Mausklick auf das Symbol das mögliche Zielsystem abgelesen und die Verbindung auf-

gebaut oder getrennt werden, bzw. bei abgebauter Verbindung der Monitor auch beendet werden.)



Das Beenden des Monitors ist nur noch über das Hauptmenü “Verbindung – Beenden” möglich.

4.4.8 Nach Verbindungsaufbau minimieren

Ist dieser Menüpunkt aktiviert, so wird der Monitor nach erfolgreichem Verbindungsaufbau automatisch minimiert, nicht jedoch beendet.

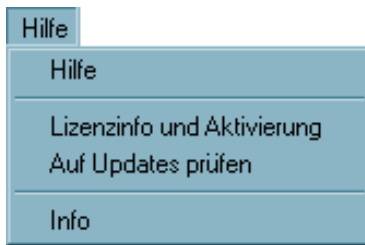


Das Beenden des Monitors ist nur über das Hauptmenü “Verbindung – Beenden” möglich.

4.4.9 Sprache

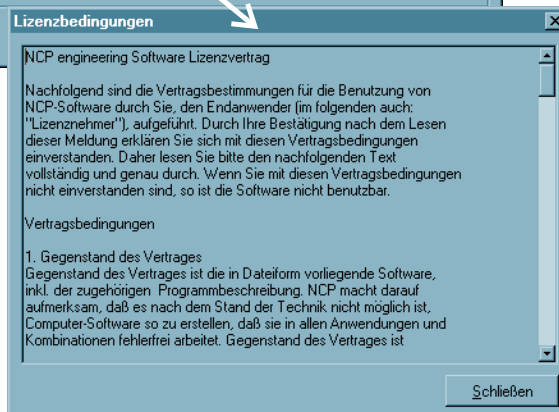
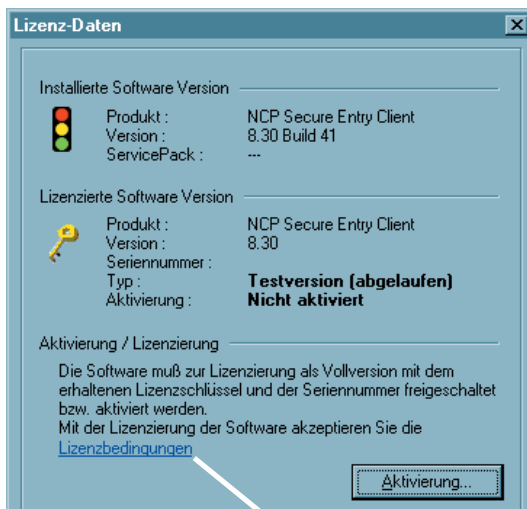
Die IPSec Client Software ist mehrsprachig angelegt. Die Standardsprache bei Auslieferung ist Deutsch. Um eine andere Sprache zu wählen, klicken Sie “Language / Sprache” im Pulldown-Menü Fenster und wählen die gewünschte Sprache.

4.5 Hilfe



Unter dem Menüpunkt “Hilfe” kann die Online-Hilfe kontextunabhängig mit Inhaltsverzeichnis und Index geöffnet werden. Außerdem kann hier der Lizenzschlüssel eingegeben und die Versionsnummer der Software abgelesen werden.

4.5.1 Lizenzinfo und Aktivierung



Unter dem Menüpunkt Lizenzinfo und Aktivierung wird die eingesetzte Software-Version und gegebenenfalls die lizenzierte Version mit Seriennummer angezeigt.

Wir die Software als Testversion eingesetzt, so kann die verbliebene Dauer der Gültigkeit im Popup abgelesen werden.

Um eine zeitlich unbegrenzt gültige Vollversion nutzen zu können, muss die Software mit dem erhaltenen Lizenzschlüssel und der Seriennummer freigeschaltet werden.

Mit der Aktivierung der Software akzeptieren Sie die Lizenzbedingungen, die nach einem Klick eingesehen werden können.

Die Aktivierung kann wahlweise online oder offline erfolgen. Beachten Sie dazu den Handbuchabschnitt “Lizenzierung”.

Die Eingabe von Lizenzschlüssel und Seriennummer kann erfolgen, nachdem Sie auf den Aktivierungsbutton geklickt haben.

Korrekt eingegebene Lizenzdaten können zu einem späteren Zeitpunkt an dieser Stelle nicht mehr ausgelesen werden.

4.5.2 Auf Updates prüfen



Unter diesem Menüpunkt kann geprüft werden, ob für die Software (auch Testversionen) mögliche Updates zur Verfügung stehen. Beachten Sie dazu weiter unten den Handbuchabschnitt “Updates”.

4.5.3 Info



Das Info-Fenster zeigt die Produktbezeichnung und die Versionsnummer Ihrer eingesetzten Software.

4.6 Lizenzierung

Im Monitormenü “Hilfe” wird unter dem Menüpunkt “Lizenzinfo und Aktivierung” die eingesetzte installierte Software-Version und gegebenenfalls die lizenzierte Software-Version mit Seriennummer angezeigt.

Die Client-Software wird zunächst immer als Testversion installiert, sofern noch keine Client-Software installiert wurde oder aber mit einer bereits installierten älteren Version noch keine Software-Aktivierung stattgefunden hat. Dies gilt auch für den Fall, wenn die ältere Version bereits lizenziert wurde – dann nämlich wird diese Version auf den Status einer Testversion zurückgesetzt, und die Lizenzdaten müssen innerhalb von 30 Tagen nochmals über den Aktivierungs-Dialog eingegeben werden.



Die verbliebene Zeitdauer bis zur Software-Aktivierung, d.h. die Gültigkeitsdauer der Testversion, wird in der Hinweisleiste des Monitors neben dem Aktivierungs-Button angezeigt (Bild links).

Um eine zeitlich unbegrenzt gültige Vollversion nutzen zu können, muss die Software mit dem erhaltenen Lizenzschlüssel und der Seriennummer im Aktivierungs-Dialog freigeschaltet werden. Mit der Aktivierung akzeptieren Sie die Lizenzbedingungen, die Sie nach einem Klick auf den entsprechenden Button einsehen können.

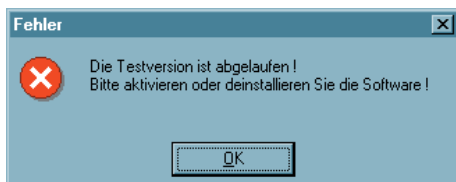
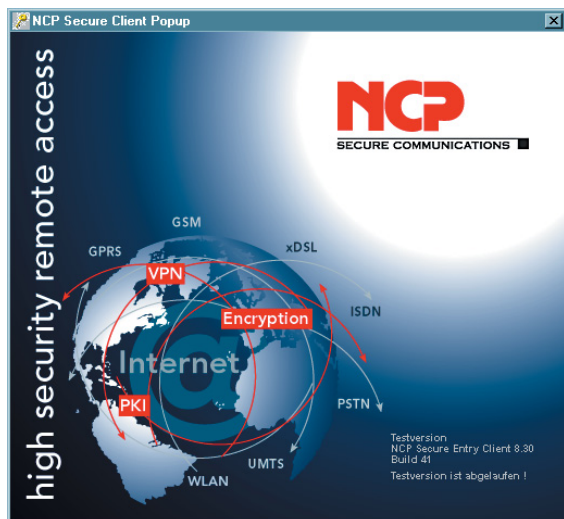
Der Aktivierungs-Dialog kann sowohl über den Aktivierungs-Button in der Hinweisleiste des Monitors als auch über das Monitormenü “Hilfe / Lizenzinfo und Aktivierung” geöffnet werden. Im folgenden können die Lizenzdaten wahlweise online oder offline über einen Assistenten eingegeben werden.

In der Offline-Variante muss eine Datei, die nach Eingabe von Lizenzschlüssel und Seriennummer erzeugt wird, an den NCP Web Server geschickt werden und der daraufhin auf der Website angezeigte Aktivierungsschlüssel notiert werden. Dieser Aktivierungsschlüssel kann zu einem späteren Zeitpunkt im Lizenzierungsfenster des Monitormenüs eingegeben werden.

In der Online-Variante werden die Lizenzierungsdaten über einen Assistenten unmittelbar nach Eingabe an den Web Server weitergegeben und die Software damit unverzüglich freigeschaltet.

4.6.1 Gültigkeitsdauer der Testversion

Die Gültigkeitsdauer der Testversion beträgt 30 Tage. Ohne Software-Aktivierung bzw. Lizenzierung ist nach dieser Zeitspanne kein Verbindungsaufbau mehr möglich.



Ab dem Zeitpunkt der Installation wird bei jedem Start der Software die Gültigkeitsdauer im Popup-Fenster angezeigt (Bild links). Darüber hinaus wird in einer Fußzeile des Monitors eingeblendet wie lange die Testversion noch verwendet werden kann und in einer Message-Box, ab der verbliebenen Zeitspanne der Gültigkeit von 10 Tagen, nachdrücklich darauf aufmerksam gemacht, dass die Software noch nicht lizenziert ist. Diese Message-Box erscheint einmalig pro Tag.

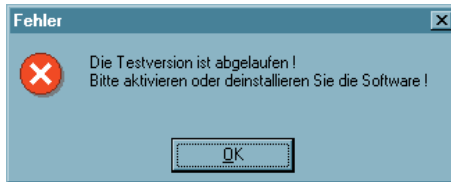
Ist die Testphase abgelaufen, können mit der Entry Client Software nur noch Verbindungen zu Zielsystemen aufgebaut werden, die der Software-Aktivierung/-Lizenzierung dienen. So kann eines der Profile des Entry Clients dazu verwendet werden, eine Internet-Verbindung zum Zweck der Lizenzierung aufzubauen. Oder eine Verbindung zum NCP Secure Enterprise Management wird hergestellt, um eine lizenzierte Version der Software herunterzuladen.

Die Aktivierung der Client Software unter Windows Vista setzt voraus, dass Sie über einen Lizenzschlüssel verfügen, der mindestens der Version 9.0 entspricht.

Sofern Ihnen ein kostenfreies Update auf die Version 9.0 zur Verfügung steht, erhalten Sie den zugehörigen Lizenzschlüssel, wenn Sie eine Software-Aktivierung durchführen.

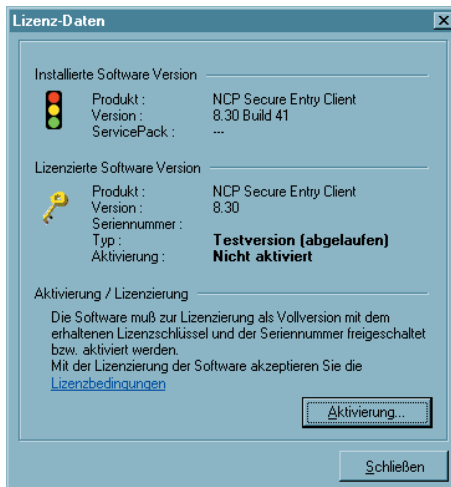
Für ein kostenpflichtiges Update auf die Version 9.0 wenden Sie sich bitte an Ihren Reseller.

4.6.2 Software-Aktivierung



Spätestens wenn die Testphase abgelaufen ist, muss die Software aktiviert oder deinstalliert werden.

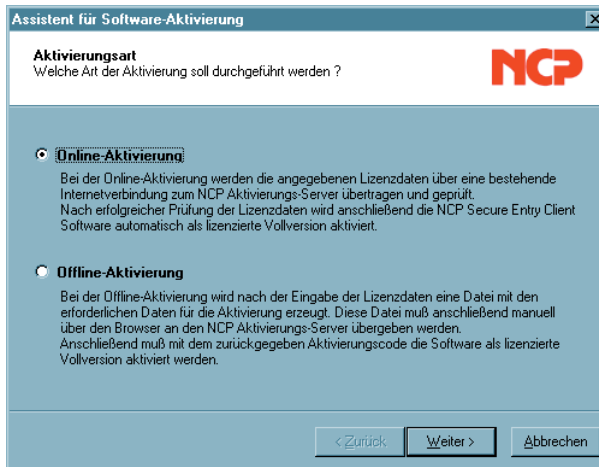
Zur Aktivierung selektieren Sie im Monitorermenü "Hilfe" den Menüpunkt "Lizenzinfo und Aktivierung".



Sie können hier ablesen um welche Software-Version es sich handelt und wie die Software lizenziert ist, d.h. dass die Testversion abgelaufen und die Software noch nicht aktiviert/lizenziert ist.

Mit Klick auf die Lizenzbedingungen wird der entsprechende Vertragstext eingeblendet. Mit der Aktivierung/Lizenzierung der Software akzeptieren Sie die Lizenzbedingungen.

Zur Aktivierung der Software klicken Sie auf den Button "Aktivierung".



Im folgenden Fenster können Sie zwischen einer Online- und einer Offline-Variante wählen.

In der Offline-Variante muss eine Datei, die nach Eingabe von Lizenzschlüssel und Seriennummer erzeugt wird, an den NCP Web Server geschickt werden und der daraufhin auf der Website angezeigte Aktivierungsschlüssel notiert werden. In der Online-Variante werden die Lizenzierungsdaten über einen Assistenten unmittelbar nach Eingabe an den Web Server weitergegeben und die Software damit unverzüglich freigeschaltet.

Nach der Wahl der Aktivierungsart werden die Lizenzdaten in die dafür vorgesehenen Felder eingetragen. Klicken Sie anschließend auf “Weiter”.

■ Online-Variante

Bei der Online-Aktivierung werden die Lizenzdaten über eine Internetverbindung zum NCP Aktivierungs-Server übertragen. Diese Internetverbindung kann entweder über den DFÜ-Dialer oder DSL hergestellt werden oder über den Entry Client.



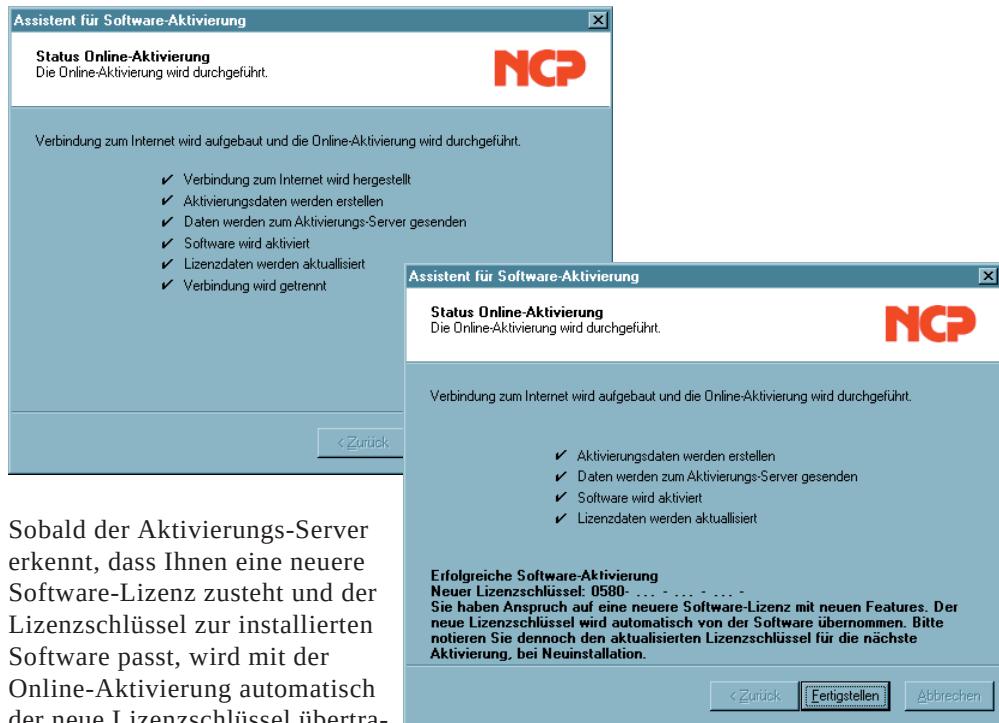
Soll die Internetverbindung nicht über den Entry Client hergestellt werden, so muss die Verbindung zunächst hergestellt werden, um anschließend über das Menü “Hilfe / Lizenzinfo und Aktivierung” den Aktivierungs-Assistenten zu starten.

Soll der Entry Client zum Verbindungsaufbau ins Internet genutzt werden (Bild links), so muss zunächst ein geeignetes Profil für den Entry Client hergestellt werden. Dabei ist darauf zu achten, dass bei aktivierter Firewall der Port 80 (für HTTP) freigeschaltet ist. (Sollte ein Proxy Server im Betriebssystem konfiguriert sein, können dessen Einstellungen nach Klick auf “Proxy-Einstellungen” übernommen werden.)

Nachdem das Profil selektiert wurde, klicken Sie auf “Weiter”.

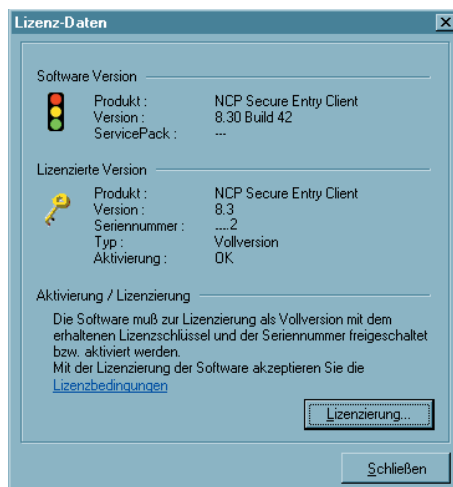
Die Internetverbindung über den Entry Client muss nicht eigens vor der Aktivierung aufgebaut werden. Sie wird automatisch aufgebaut, nachdem das gewünschte, bestehende Profil im Assistenten für Software-Aktivierung ausgewählt wurde und der Button "Weiter" angeklickt wird.

Die Software-Aktivierung erfolgt automatisch in der angegebenen Reihenfolge.



Sobald der Aktivierungs-Server erkennt, dass Ihnen eine neuere Software-Lizenz zusteht und der Lizenzschlüssel zur installierten Software passt, wird mit der Online-Aktivierung automatisch der neue Lizenzschlüssel übertragen (Lizenz-Update) und damit die neuen Features der Software freigeschaltet.*

* Bitte beachten Sie dazu den Abschnitt "Updates" am Ende dieses Kapitels.



Nach Abschluss der Aktivierung kann im Fenster für die Lizenzdaten abgelesen werden, dass es sich bei der eingesetzten Software um eine korrekt aktivierte Vollversion handelt.

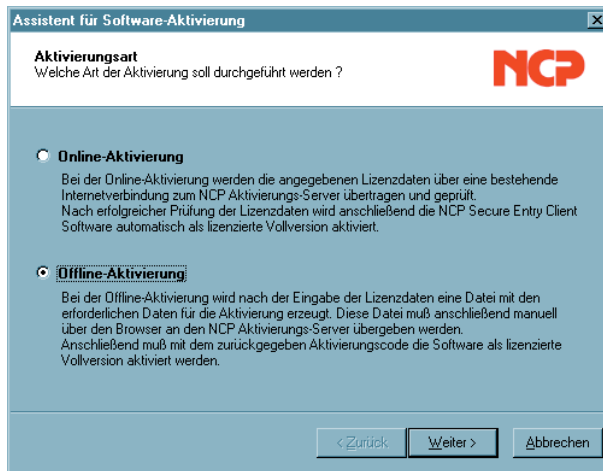
Die Nummer der Software-Version und der lizenzierten Version sollten übereinstimmen, ansonsten muss mit einem neueren Lizenzschlüssel die Lizenz aktualisiert werden. Dazu klicken Sie den Button "Lizenzierung". Beachten Sie dazu auch die Beschreibung am Ende der Offline-Variante.

■ Offline-Variante

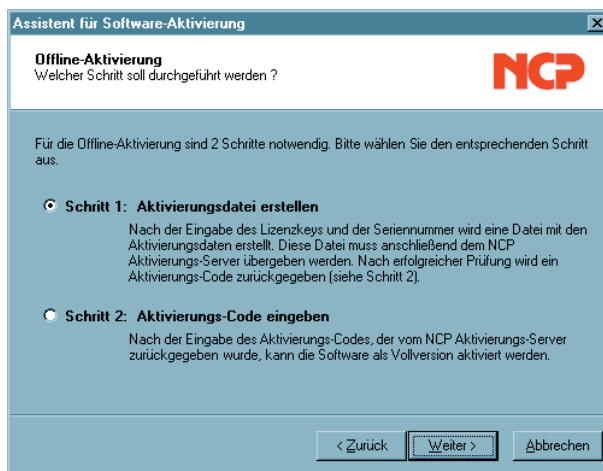
Die Offline-Variante wird in zwei Schritten durchgeführt. Im ersten Schritt muss eine Datei, die nach Eingabe von Lizenzschlüssel und Seriennummer erzeugt wird, an den NCP Web Server geschickt werden. Die URL lautet:

`http://www.ncp.de/deutsch/services/license`

Auf der Website wird daraufhin ein Aktivierungsschlüssel angezeigt, der notiert werden muss, um im zweiten Schritt, der auch zu einem späteren Zeitpunkt vorgenommen werden kann, im Lizenzierungsfenster des Monitormenüs eingegeben werden zu können.



Die Offline-Variante wird über das Monitormenü "Hilfe / Lizenzinfo und Aktivierung" gestartet und im ersten Fenster des Aktivierungs-Assistenten selektiert. Klicken Sie auf "Weiter" ...



Im zweiten Fenster des Aktivierungs-Assistenten werden die beiden Schritte der Offline-Aktivierung erklärt. Der erste Schritt, die Erstellung der Aktivierungsdatei, ist automatisch selektiert. Klicken Sie auf den Button mit "Weiter" ...

Im folgenden Fenster geben Sie die Lizenzdaten ein und klicken auf "Weiter" ...

Geben Sie nun Name und Pfad für die Aktivierungsdatei ein (z.B. auf dem Desktop). Standardmäßig wird das Installationsverzeichnis der Software und der Name ActiData.txt (mit Seriennummer) eingesetzt.

Nun wird die Aktivierungsdatei erstellt, die an den Aktivierungs-Server übergeben werden muss.

Dazu muss die NCP Website aufgerufen werden:

<http://www.ncp.de/deutsch/services/license>

Partner - Area

Knowledgebase

IPSec Kompatibilität

CE Kompatibilität

Mobile Connect Cards Kompatibilität

Software - Aktivierung

Offline - Aktivierung

FAQ zur Aktivierung

Update - Schlüssel

Trainings

Hotline Support

Feedback

NCP Secure Communications Software

Aktivierung



Software-Aktivierung

Bitte kopieren Sie den Inhalt der vom NCP Secure Client erzeugten Aktivierungsdatei (**Offline-Aktivierung, Schritt 1**) in das dafür vorgesehene Textfeld. Anschließend klicken Sie bitte auf den Knopf "Absenden", um die Daten zu unserem Aktivierungs-Server zu übertragen.

Alternativ können Sie die Aktivierungsdatei auch direkt zum Aktivierungs-Server hochladen. Hierfür klicken Sie auf den Knopf "Durchsuchen..." und wählen anschließend die Datei mit den Aktivierungsdaten aus. Danach klicken Sie bitte auf den Knopf "Absenden", um die Datei zu unserem Aktivierungs-Server zu übertragen.

Nach dem Absenden der Aktivierungsdaten bzw. der Datei erhalten Sie einen **Aktivierungs-Code**. Bitte setzen Sie nun die Software-Aktivierung im NCP Entry Client fort, indem Sie das Monitor-Menü öffnen (Hilfe -> Lizenzinfo und Aktivierung -> Offline-Aktivierung). Unter **Schritt 2** wird der im folgenden angezeigte **Aktivierungs-Code** abgefragt. Nach diesem Schritt ist die Software-Aktivierung abgeschlossen.

Inhalt der Aktivierungsdatei :

Dateiname :

Durchsuchen...

Absenden

Zurücksetzen

🔍 ? @ 📞

high security remote access

Die Datenübergabe von der Aktivierungsdatei an den Aktivierungs-Server kann auf zweierlei Weise erfolgen. Entweder kopieren Sie den Inhalt der Aktivierungsdatei mit Copy&Paste, nachdem Sie die Aktivierungsdatei mit dem Notepad (ASCII-Editor) geöffnet haben, in das auf der Website geöffnete Fenster "Inhalt der Aktivierungsdatei" oder Sie klicken auf den Button "Durchsuchen" und selektieren die Aktivierungsdatei. Anschließend klicken Sie auf "Absenden".



SECURE COMMUNICATIONS

[Home](#) [Unternehmen](#) [Security](#) [Produkte](#) [Vertrieb](#) [Services](#) [Presse](#)
[Sitemap](#)

[Partner - Area](#)
[Knowledgebase](#)
[IPSec Kompatibilität](#)
[CE Kompatibilität](#)
[Mobile Connect Cards Kompatibilität](#)
[Software - Aktivierung](#)
[Offline - Aktivierung](#)
[FAQ zur Aktivierung](#)
[Update - Schlüssel](#)
[Trainings](#)
[Hotline Support](#)
[Feedback](#)

Neuer Aktivierungs-Code

Aktivierungs-Code: TITXTE

Neuer Lizenzschlüssel: 005

Der Aktivierungs-Code konnte erfolgreich generiert werden. In unserem System wurde jedoch festgestellt, dass Sie Anspruch auf eine neuere Software-Lizenz besitzen. Wenn Sie die neuesten Features aktivieren möchten, führen Sie die Aktivierung zu Ende und verwenden anschließend den oben angezeigten Lizenzschlüssel.

Um die Software-Aktivierung zu beenden, notieren Sie sich den oben gezeigten Aktivierungs-Code und setzen die Aktivierung mit der **Offline-Aktivierung** unter dem Menü-Punkt "Hilfe → Lizenzinfo und Aktivierung" fort **Schritt 2**. Nach Abschluss der Aktivierung können Sie unter dem gleichen Menü-Punkt "Hilfe → Lizenzinfo und Aktivierung" den neuen Lizenzschlüssel eingeben.

E-Mail: support@ncp.de

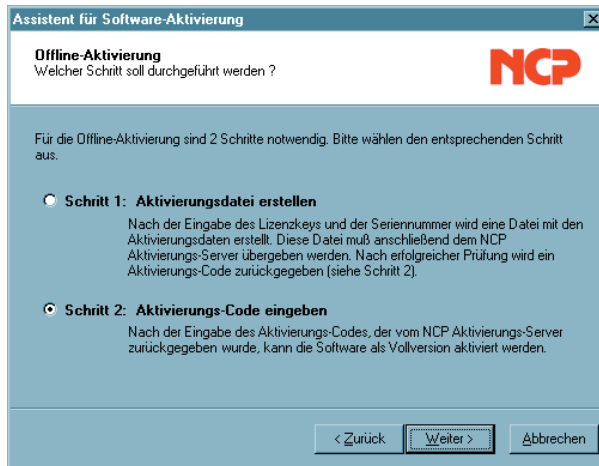
Telefon: 0900-1996800 (ca. 80 Euro / Minute)



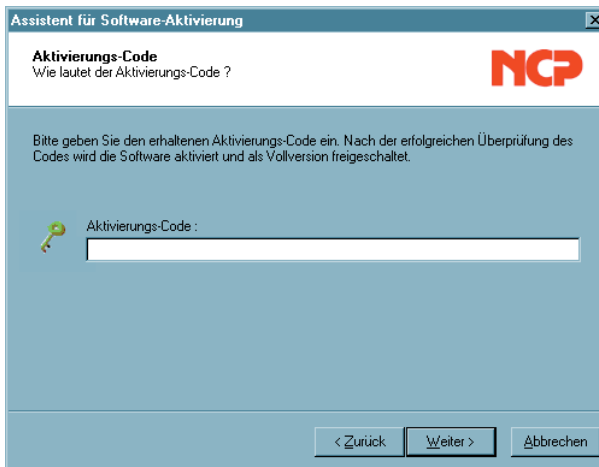
high security remote access

Daraufhin wird der Aktivierungs-Code generiert und auf der Website angezeigt. Notieren Sie sich den Aktivierungs-Code und setzen Sie die Aktivierung fort unter dem Menüpunkt "Hilfe / Lizenzinfo und Aktivierung", indem Sie in der Offline-Variante den zweiten Schritt der Aktivierung ausführen.

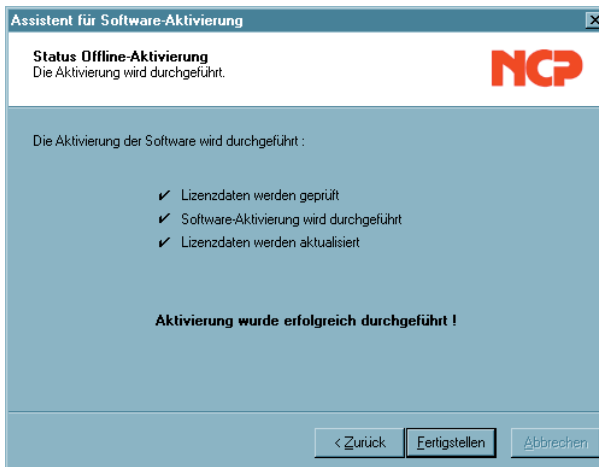
Sollte der Aktivierungs-Server erkennen, dass Ihnen eine neuere Software-Lizenz zusteht und der Lizenzschlüssel zur installierten Software passt, wird mit der Online-Aktivierung automatisch der neue Lizenzschlüssel angezeigt. Wenn Sie die neuen Features aktivieren möchten, notieren Sie sich den neuen Lizenzschlüssel, führen Sie die Aktivierung zu Ende und verwenden anschließend den neuen Lizenzschlüssel. (Bitte beachten Sie dazu den Abschnitt "Szenarien" am Ende dieses Kapitels.)



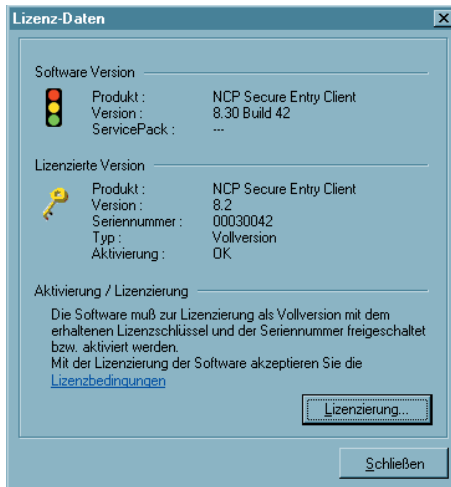
Der zweite Schritt der Offline-Variante wird über das Monitormenü “Hilfe / Lizenzinfo und Aktivierung” angestoßen. Nachdem die Offline-Variante gewählt wurde, selektieren Sie den zweiten Schritt.



Daraufhin öffnet sich ein Fenster des Aktivierungs-Assistenten zur Eingabe des Aktivierungs-Codes. Wenn Sie ihn eingetragen haben, können Sie “Weiter” klicken.



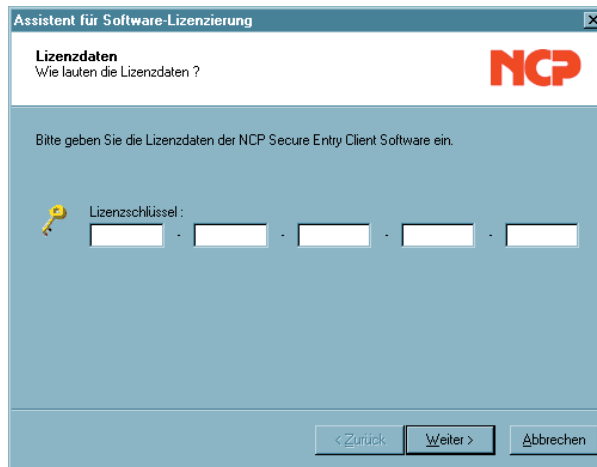
Mit dem folgenden Fenster wird die Offline-Aktivierung abgeschlossen.



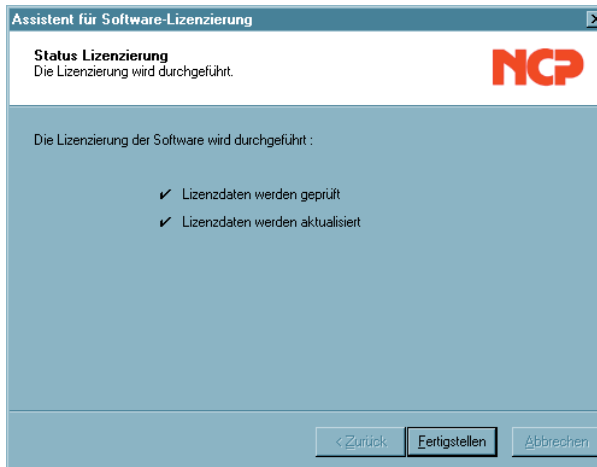
Nach Abschluss der Aktivierung kann im Fenster für die Lizenzdaten abgelesen werden, dass es sich bei der eingesetzten Software um eine korrekt aktivierte Vollversion handelt.

Die Nummer der Software-Version und der lizenzierten Version können sich unterscheiden, sofern die Lizenzierung nur für eine ältere Version gültig ist.

Sollten Sie vom Aktivierungs-Server während der Offline-Aktivierung einen neuen Lizenzschlüssel erhalten haben (siehe oben bei Anzeige des Aktivierungs-Codes), so geben Sie diesen Lizenzschlüssel für ein Lizenz-Update ein, indem Sie den Button "Lizenzierung" klicken.

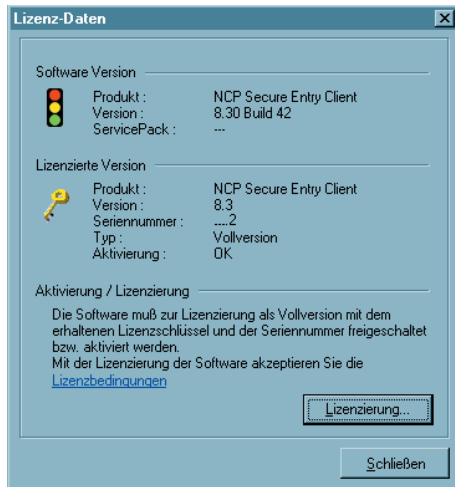


In dem folgenden Fenster des Assistenten geben Sie den neuen Lizenzschlüssel ein und klicken auf "Weiter".



Die Lizenzdaten werden geprüft und übernommen.

Klicken Sie "Fertigstellen" wenn die Prüfung abgeschlossen ist.



Im Fenster mit den Lizenzdaten sehen Sie nun, dass die Nummer der Software-Version und der lizenzierten Version übereinstimmen.

4.7 Updates

Unter dem Menüpunkt “Auf Updates prüfen”, im Monitormenü unter “Hilfe”, kann geprüft werden, ob bei NCP eine neuere Software vorliegt, als die von Ihnen installierte. Dies ist auch dann möglich, wenn eine Testversion installiert wurde. Liegt eine neuere Version bei NCP vor, so ist immer ein Software-Update möglich. Informationen zum Leistungsumfang der neuesten Software erhalten Sie ständig unter der Website:

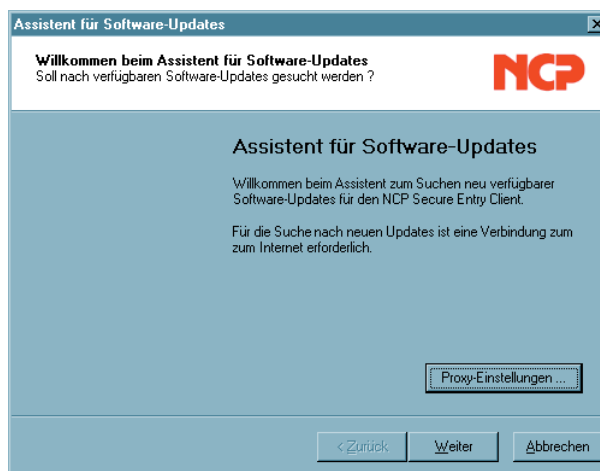
<http://www.ncp.de/deutsch/services/whatsnew/index.html>

Das Software-Update ist immer dann kostenpflichtig, wenn es sich bei der neueren Version um ein Major Release handelt, erkennbar an der Änderung der ersten Dezimalstelle hinter dem Komma. Zum Beispiel: Ist eine Version 8.26 installiert und die nächste Software-Version hat die Nummer 8.3, so ist ein Software-Update von 8.26 auf 8.3, sowie insbesondere die Nutzung der neuen Features, kostenpflichtig. Die neuen Features können nur genutzt werden, wenn die neue Software nach Installation mit einem neuen Lizenzschlüssel aktiviert wurde, wie oben unter Software-Aktivierung beschrieben. Der neue Lizenzschlüssel wird erzeugt, indem Seriennummer und Update-Schlüssel, der über den Reseller vorort erworben werden kann, auf folgender Website eingetragen werden:

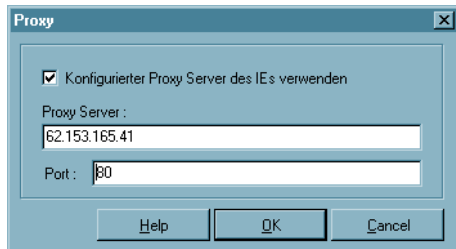
<http://www.ncp.de/deutsch/services/updkeys/index.html>

Das Software-Update ist immer dann kostenfrei, wenn es sich bei der neueren Version um ein Service Release handelt, erkennbar an der Änderung der zweiten Dezimalstelle hinter dem Komma. Zum Beispiel: Ist eine Version 8.26 installiert und die nächste Software-Version hat die Nummer 8.27, so ist ein Software-Update von 8.26 auf 8.27, sowie insbesondere die Nutzung der neuen Features, kostenfrei. Die neuen Features können ohne Aktivierung durch einen 8.2x Lizenzschlüssel genutzt werden, sobald die neue Software installiert wurde. Ein Service Release beinhaltet unter anderem Bugfixes, eine Erweiterung der Hardware-Unterstützung und Kompatibilitätserweiterungen.

4.7.1 Software-Updates

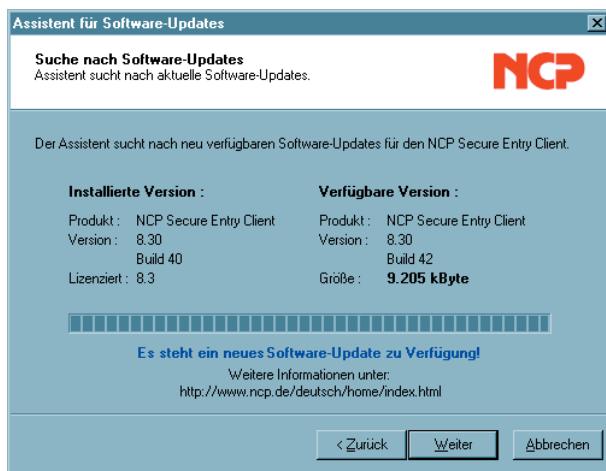


Nachdem Sie den Menüpunkt “Auf Updates prüfen” selektiert haben, erhalten Sie das nebenstehende Fenster. Um auf neue Updates prüfen zu können, benötigen Sie eine Verbindung ins Internet. Soll der Entry Client zum Verbindungsaufbau ins Internet genutzt werden, so ist darauf zu achten, dass bei aktivierter Firewall der Port 80 (für HTTP) freigeschaltet ist.



Sollte ein Proxy Server im Betriebssystem konfiguriert sein, können diese Einstellungen übernommen werden.

Wenn die Proxy-Einstellungen korrekt konfiguriert sind, klicken Sie auf "OK". Der Assistent sucht nun über die Internet-Verbindung nach neu verfügbaren Software-Updates.



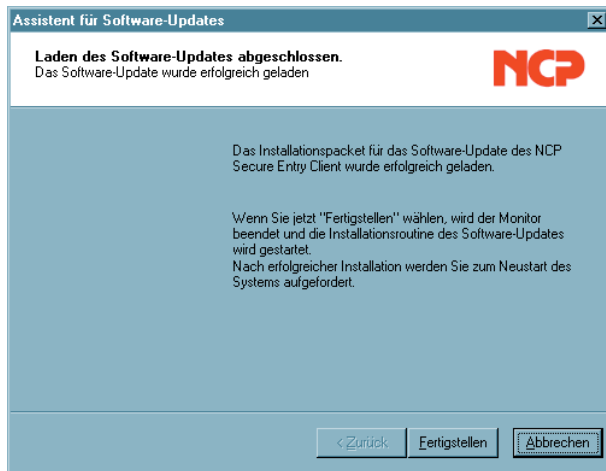
Steht ein Software-Update zur Verfügung, wird es in nebenstehendem Fenster angezeigt.

(In diesem Fall unterscheidet sich die Version nur durch die Build-Nummer.)

Klicken Sie auf "Weiter", wenn Sie die aktuellere Software nutzen wollen.

Die neuen Features sind beschrieben unter:

<http://www.ncp.de/deutsch/services/whatsnew/index.html>



Damit wird das Installationspaket für die neueste Software heruntergeladen.

Mit Klick auf "Fertigstellen" wird der Monitor beendet und die Installation des Software-Updates gestartet.

Nach Start des Installshield Wizzard wählen Sie wie bei der Standardinstallation die Installationssprache und beantworten anschließend die Update-Frage mit "Ja". Danach wird die Installation automatisch durchgeführt. Sie ist abgeschlossen, wenn Sie den Rechner neu gestartet haben.



5. Konfigurationsparameter

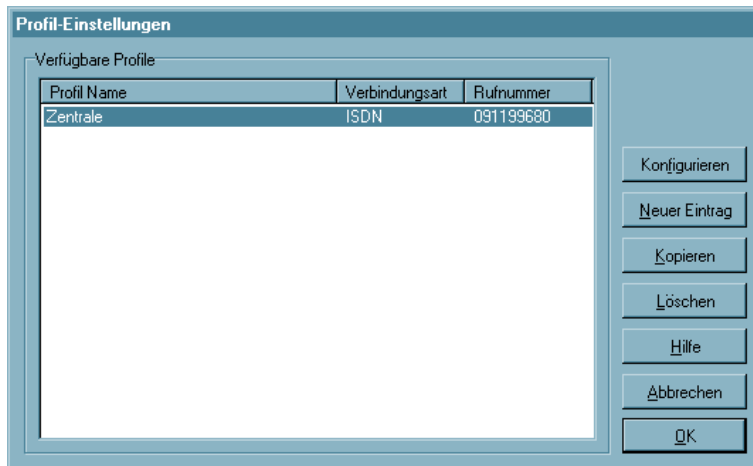


Die IPSec Client Software gestattet die Einrichtung individueller Profile für entsprechende Zielsysteme, die nach den Benutzeranforderungen konfiguriert werden können.

Im folgenden sind alle Parameterbeschreibungen aufgeführt, und sie sind so angeordnet, wie sie auf der Oberfläche des Client Monitors erscheinen.

5.1 Profil-Einstellungen

Nachdem Sie “Profil-Einstellungen” im Menü des Monitors angeklickt haben, öffnet sich das Menü und zeigt eine Übersicht über die bereits definierten Profile und die Rufnummern der zugehörigen Ziele.



Seitlich finden Sie Buttons, über die Sie die Einträge des Telefonbuchs (Zielsysteme) modifizieren können.

Um ein neues Profil zu definieren, klicken Sie in der Menüleiste des Monitors auf “Profil-Einstellungen”. Das Menü öffnet sich nun und zeigt die bereits definierten Profile. Klicken Sie jetzt auf “Neuer Eintrag”. Jetzt legt der “Assistent für ein neues Profil” mit Ihrer Hilfe ein neues an. Dazu blendet er die unbedingt notwendigen Parameter auf. Wenn Sie die Einträge in diesen Feldern vorgenommen haben, ist ein neues Profil angelegt. Für alle weiteren Parameterfelder werden Standardwerte eingetragen.

Um diese Standardwerte zu editieren, d.h. weitere Parameter so einzustellen, wie es den Verbindungsanforderungen zum zugehörigen Zielsystem entspricht, wählen Sie mit der Maus das Profil aus, dessen Werte Sie ändern möchten und klicken anschließend auf “Konfigurieren”.

Um die Definitionen eines bereits definierten Profils zu kopieren, klicken Sie “Kopieren”.

Um ein Profil zu löschen, wählen Sie es aus und klicken “Löschen”.

Parameterfelder:

Die Parameter, die die jeweilige Verbindung über das Profil zu den Zielen spezifizieren, sind in verschiedenen Parameterfeldern gesammelt. In der Kopfzeile steht der Name des Profils (siehe auch →Profil-Einstellungen, Konfigurieren). Seitlich sind die Titel der Parameterfelder angeordnet:

- 1 *Grundeinstellungen*
- 2 *Netzeinwahl*
- 3 *HTTP-Anmeldung*
- 4 *Modem*
- 5 *Line Management*
- 6 *IPSec-Einstellungen*
- 7 *Erweiterte IPSec-Optionen*
- 8 *Identität*
- 9 *IP-Adressen-Zuweisung*
- 10 *VPN IP-Netze*
- 11 *Zertifikats-Überprüfung*
- 12 *Link Firewall*



5.1.1 Grundeinstellungen



Im Parameterfeld “Grundeinstellungen” wird der “Profil-Name”, den “Verbindungstyp” und das “Verbindungsmedium” zu einem Profil eingegeben.

Parameter:

- ☐ Profil-Name
- ☐ Verbindungstyp
- ☐ Verbindungsmedium
- ☐ Profil für automatische Medienerkennung verwenden
- ☐ Dieses Profil nach jedem Neustart des Systems verwenden
- ☐ Benutze Microsoft DFÜ-Dialer

■ Profil-Name

Wenn Sie ein neues Profil definieren, sollten Sie zunächst einen unverwechselbaren Namen für dieses System eintragen (z.B. IBM London). Der Name des Profils darf jeden gewünschten Buchstaben wie auch Ziffern beinhalten und darf, Leerzeichen mitgezählt, bis zu 39 Zeichen lang sein.

■ Verbindungstyp

Alternativ stehen mit dem IPSec Client zwei Verbindungstypen zur Wahl:

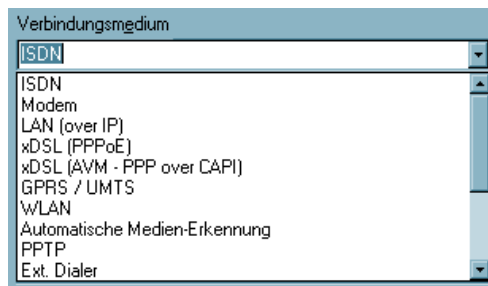
VPN zu IPSec-Gegenstelle

In diesem Fall wählen Sie sich mit dem IPSec Client in das Firmennetz ein (bzw. an das Gateway an). Dazu wird ein VPN-Tunnel aufgebaut.

Internet-Verbindung ohne VPN

In diesem Fall nutzen Sie den IPSec Client nur zur Einwahl in das Internet. Dabei wird Network Address Translation (IPNAT) weiterhin im Hintergrund genutzt, sodass nur Datenpakete akzeptiert werden, die angefordert wurden.

■ Verbindungsmedium



Das Verbindungsmedium kann für jedes Profil eigens eingestellt werden, vorausgesetzt Sie haben die entsprechende Hardware angeschlossen und in Ihrem (Windows-)System installiert.

ISDN

Angeschlossene Hardware: ISDN-Hardware mit Capi 2.0-Unterstützung;

Netze: ISDN-Festnetz;

Gegenstellen: ISDN-Hardware;

Modem

Angeschlossene Hardware: Asynchrone Modems (PCMCIA-Modem, GSM-Karte) mit Com Port-Unterstützung;

Netze: Analoges Fernsprechnetz (PSTN) (auch GSM);

Gegenstellen: Modem oder ISDN-Karte mit digitalem Modem;

LAN (over IP)

Angeschlossene Hardware: LAN-Adapter;

Netze: Local Area Network mit Ethernet oder Token Ring;

Gegenstellen: Die Gegenstellen des lokalen Multiprotokoll-Routers im LAN;

xDSL (PPPoE)

Angeschlossene Hardware: Ethernet-Adapter, xDSL-Modem;

Netze: xDSL;

Gegenstellen: Access-Router im xDSL;

xDSL (AVM - PPP over CAPI)

Diese Verbindungsart kann gewählt werden, wenn eine AVM Fritz! DSL-Karte eingesetzt wird. Im Feld "Rufnummer (Ziel)" in der Gruppe "Netzeinwahl" können für die Verbindung über CAPI noch AVM-spezifische Initialisierungskommandos eingetragen werden. Unter Windows Betriebssystemen wird jedoch empfohlen den Standard "xDSL (PPPoE)" zu verwenden, da damit direkt über die Netzwerkschnittstelle mit der Karte kommuniziert wird. Bei Verwendung der AVM Fritz! DSL-Karte wird keine separate zusätzliche Netzwerkkarte benötigt.

Netze: xDSL;

Gegenstellen: Access-Router im xDSL;



Bitte beachten Sie, dass je nach gewählter Verbindungsart die dafür erforderliche Hardware und ggf. die Treiber dazu installiert sein müssen.

GPRS / UMTS

Dieses Einwahlmedium wählen Sie, wenn die Einwahl über das Mobilfunknetz (GPRS oder UMTS) erfolgen soll. Beachten Sie dazu den Hinweis unter den Installationsvoraussetzungen zu "Analoges Modem".

PPTP

Microsoft Point-to-Point Tunnel Protocol;

Angeschlossene Hardware: Ethernet-Adapter, xDSL-Modem;

Netze: xDSL;

Gegenstellen: Access-Router im xDSL;

WLAN

Hardware: WLAN-Adapter;
 Netze: Funknetz;
 Gegenstellen: Access Point;



Unter Windows 2000/XP/Vista kann der WLAN-Adapter mit der Verbindungsart "WLAN" betrieben werden. Im Monitormenü erscheint eigens der Menüpunkt "WLAN-Einstellungen", worin die Zugangsdaten zum Funknetz in einem Profil hinterlegt werden können. Wird diese "WLAN-Konfiguration aktiviert", so muss das Management-Tool der WLAN-Karte deaktiviert werden. (Alternativ kann auch das Management-Tool der WLAN-Karte genutzt werden, dann muss die WLAN-Konfiguration im Monitormenü deaktiviert werden.)

Wird die Verbindungsart WLAN für ein Zielsystem im Telefonbuch eingestellt, so wird unter dem grafischen Feld des Client-Monitors eine weitere Fläche eingeblendet, auf der die Feldstärke und das WLAN-Netz dargestellt werden (siehe →WLAN-Einstellungen).

Ext. Dialer

Ist die Verbindungsart "Ext.Dialer" (über externen Dialer) eingestellt, wird beim Drücken des "Verbinden"-Buttons eine vorkonfigurierte EXE-Datei (z.B. der iPass-Dialer) gestartet. Über diese EXE-Datei wird die Verbindung zum Internet hergestellt und anschließend über "RWSCMD/connect" der VPN-Verbindungsaufbau des Clients angestoßen. Der NCP Dialer arbeitet unter dieser Konfiguration im LAN-Modus.



Diese Verbindungsart funktioniert nur, wenn im Parameterfeld "Verbindungssteuerung" der Verbindungsaufbau auf "manuell" geschaltet wird.

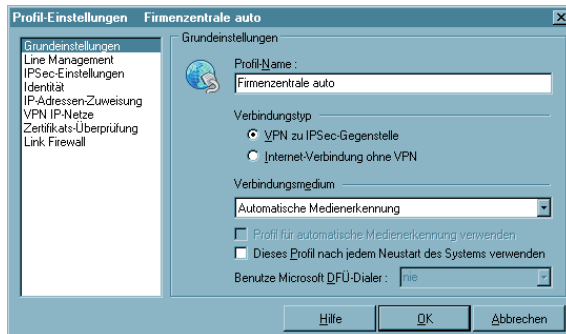
Je nach installiertem Dialer (iPass oder T-Online) muss in der Konfigurationsdatei EXTDIAL.INI für den Eintrag "ExeName" die EXE-Datei des Dialers eingetragen werden. Um nicht den kompletten Pfad für den Dialer in der DAT-Datei angeben zu müssen, kann optional der Pfad aus der Registry gelesen und in die INI-Datei eingetragen werden. Der genaue Wortlaut der Kopfzeile des Dialers, unter Beachtung der Groß- und Kleinschreibung muss in der INI-Datei unter "Caption" eingetragen werden.

Beispiel der INI-Datei für iPass (in der Registry findet sich unter "InstallPath" der Installations-Pfad des iPass-Dialers "Software\iPass\iPassConnectEngine"):

```
DialerInstallPathKey   = Software\iPass\iPassConnectEngine
DialerInstallPathValue = InstallPath
DialerExec             = iPassConnectGUI.exe
Caption               = iPassConnect
```

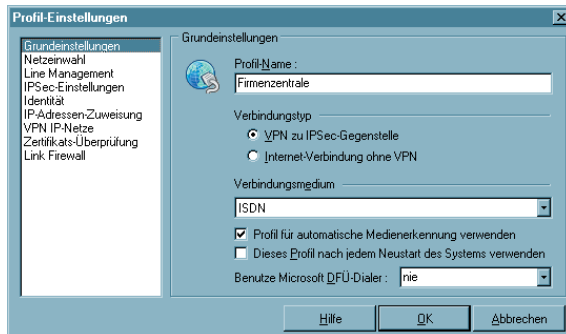
Automatische Medienerkennung

Werden wechselweise unterschiedliche Verbindungsarten genutzt, wie zum Beispiel Modem und ISDN, so kann die manuelle Auswahl des Zielsystems mit dem jeweils zur Verfügung stehenden Verbindungsmedium entfallen, wenn ein Zielsystem für “Automatische Medienerkennung” konfiguriert wurde und je ein Zielsystem mit den alternativ verfügbaren Verbindungsarten, wie zum Beispiel Modem und ISDN.



Dabei ist zu beachten, dass das Zielsystem mit automatischer Medienerkennung mit allen für die Verbindung zum VPN Gateway nötigen Parametern konfiguriert ist (Bild links oben), wohingegen die Zielsysteme mit den alternativen Verbindungsarten so konfiguriert sein müssen, dass die jeweils gewünschte Verbindungsart (evtl. auch die Modemparameter) eingestellt ist und die Funktion “Eintrag für automatische Medienerkennung” aktiviert ist (Bild links unten).

Außerdem müssen für das jeweilige Verbindungsmedium die Eingangsdaten zum ISP im Parameterfeld “Netzeinwahl” gesetzt sein.



Bei einem Verbindungsaufbau erkennt der Client automatisch, welche Verbindungsarten aktuell zur Verfügung stehen und wählt davon die schnellste aus, wobei bei mehreren alternativen Übertragungswegen automatisch der schnellste gewählt wird. In einer Suchroutine ist die Priorisierung der Verbindungsarten in folgender Reihenfolge festgelegt: 1. LAN, 2. WLAN, 3. DSL, 4. UMTS/GPRS, 5. ISDN, 6. MODEM. Die Eingangsdaten für die Verbindung zum ISP werden aus den Telefonbucheinträgen übernommen, die für die automatische Medienerkennung konfiguriert wurden.

Profil für automatische Medienerkennung verwenden



Mit Aktivierung dieser Funktion wird dieses Zielsystem an den Telefonbucheintrag für automatische Medienerkennung gebunden und bei Verfügbarkeit des entsprechenden Mediums automatisch für einen potentiellen Verbindungsaufbau herangezogen. Beachten Sie dazu die Beschreibung zur “Verbindungsart”.

Dieses Zielsystem kann auch manuell selektiert werden, um eine Verbindung herzustellen, sofern die Tunnel-Parameter für den Zugang zum VPN Gateway korrekt eingetragen sind.

■ Dieses Profil nach jedem Neustart des Systems verwenden

Normalerweise wird der Client-Monitor nach einem Neustart mit dem zuletzt genutzten Profil geöffnet. Wird diese Funktion aktiviert, wird nach einem Neustart des Systems immer das hierzu gehörige Profil geladen, unabhängig davon, welches Profil zuletzt genutzt wurde.

■ Benutze Microsoft DFÜ-Dialer

Zur Einwahl am ISP (Internet Service Provider) kann der Microsoft DFÜ-Dialer genutzt werden. Dies ist immer dann nötig, wenn der Einwahlpunkt ein Einwahl-Script benötigt. Der DFÜ-Dialer unterstützt dieses Script. Im Parameterfenster "Netzeinwahl" wird anschließend die Script-Datei unter Eingabe von Pfad und Namen zur eingespielten Script-Datei eingetragen (siehe →Script-Datei).

Mit der Einstellung "nie" wird ausschließlich der NCP Dialer zur Einwahl verwendet. Soll der DFÜ-Dialer "nur bei Script-Einwahl" verwendet werden, so wählen Sie diese Option. Bei einem Einwahlpunkt, der kein Script verlangt, wird automatisch auf den NCP Dialer umgeschaltet. Soll der DFÜ-Dialer immer verwendet werden, muss die entsprechende Einstellung vorgenommen werden.

5.1.2 Netzeinwahl



Dieses Parameterfeld beinhaltet den Benutzernamen und das Passwort, die bei der Anwahl an das Zielsystem zur Identifizierung benötigt werden. Diese beiden Größen werden auch für die PPP-Verhandlung zum ISP (Internet Service Provider) benötigt. Das Parameterfeld erscheint überhaupt nicht, wenn der IPSec Client mit dem Verbindungsmedium "LAN over IP" betrieben wird.

Parameter:

- ☐ Benutzername
- ☐ Passwort
- ☐ Passwort speichern
- ☐ Rufnummer (Ziel)
- ☐ Alternative Rufnummern
- ☐ Script-Datei

■ Benutzername

Mit dem “Benutzernamen” weisen Sie sich gegenüber dem Network Access Server (NAS) aus, wenn Sie eine Verbindung zum Zielsystem aufbauen wollen. Bei Kommunikation über das Internet benötigen Sie den Benutzernamen zur Identifikation am ISP (Internet Service Provider). Der Name für den Benutzer kann bis zu 254 Zeichen lang sein. Für gewöhnlich wird Ihnen ein “Benutzername” vom Zielsystem zugewiesen, da Sie vom Zielsystem (auch Radius- oder LDAP-Server) erkannt werden müssen. Sie erhalten ihn von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

■ Passwort

Das Passwort benötigen Sie, um sich gegenüber dem Network Access Server (NAS) ausweisen zu können, wenn die Verbindung aufgebaut ist. Das Passwort darf bis zu 254 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Passwort vom Zielsystem zugewiesen, da Sie vom Zielsystem auch erkannt werden müssen. Sie erhalten es von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Wenn Sie das Passwort eingeben, werden alle Zeichen als Stern (*) dargestellt, um sie vor ungewünschten Beobachtern zu verbergen. Es ist wichtig, dass Sie das Passwort genau nach der Vorgabe eintragen und dabei auch auf Groß- und Kleinschreibung achten.



Wird der Parameter “Passwort speichern” nicht aktiviert, so muss er bei jedem Verbindungsaufbau das Passwort per Hand eingeben.

■ Passwort speichern

Dieser Parameter muss aktiviert (angeklickt) werden, wenn gewünscht wird, dass das Passwort und das Passwort Ziel (sofern es eingegeben ist) gespeichert wird. Andernfalls werden die Passwörter gelöscht, sobald der PC gebootet wird oder ein Zielsystem gewechselt wird. Standard ist die aktivierte Funktion.



Wichtig: Bitte beachten Sie, dass im Falle gespeicherter Passwörter, jedermann mit Ihrer Client Software arbeiten kann – auch wenn er die Passwörter nicht kennt.

■ Rufnummer (Ziel)

Für jedes Ziel muss eine Rufnummer definiert sein, da der Client sonst keine Verbindung herstellen kann. Diese Rufnummer muss genauso eingetragen werden, als würden Sie diese Telefonnummer per Hand wählen. D.h. Sie müssen alle notwendigen Vorwahlziffern berücksichtigen: Landesvorwahl, Ortsvorwahl, Durchwahlziffern, etc. etc.

Tragen Sie jedoch nicht die Amtsholung ein, auch wenn Sie an einer Nebenstellenanlage angeschlossen sind! Die Amtsholung wird unter dem Monitor-Menüpunkt "Konfiguration" eingetragen und hat auf diese Weise Gültigkeit für alle Rufe (→siehe – Amtsholung).

Beispiel: Sie wollen eine Verbindung von Deutschland nach England herstellen

00 (für die internationale Verbindung, wenn Sie von Deutschland aus wählen)

44 (dies ist die landesspezifische Vorwahl für England)

171 (Vorwahl für London)

1234567 (die Nummer, die Sie zu erreichen wünschen)

Insgesamt wird nach diesem Beispiel folgende Nummer im Telefonbuch gespeichert und für die Anwahl verwendet: 00441711234567

Die Rufnummer des Ziels kann bis zu 30 Ziffern beinhalten.



Hinweis: Wenn ein Zielsystem eine Verbindung zu Ihrem PC über Rückruf aufbauen will, benötigt der Client diese Rufnummer in diesem Feld, um den Rückruf, entsprechend des gewählten Rückrufmodus annehmen zu können.

■ Alternative Rufnummern

Möglicherweise ist das Zielsystem ein Network Access Server (NAS), der mit mehreren S0-Anschlüssen für verschiedene Rufnummern ausgestattet ist. In diesen Fall empfiehlt es sich, alternative Rufnummern einzugeben – falls zum Beispiel die erste Nummer besetzt ist. Die alternativen Rufnummern werden der ersten Nummer angehängt, nur mit einem Doppelpunkt (;) oder einem Semikolon (;) getrennt.

Maximal werden 8 alternative Rufnummern unterstützt.

Beispiel : 000441711234567:000441711234568

Die erste Nummer ist die Standard-Rufnummer und wird immer zuerst gewählt. Kann keine Verbindung hergestellt werden, weil besetzt ist, wird die zweite Nummer gewählt, usw.



Wichtig: Bitte beachten Sie, dass der Verbindungsaufbau nur funktionieren kann, wenn die Protokoll-Eigenschaften für die Anschlüsse der alternativen Rufnummern die gleichen sind.

■ Script-Datei

Wenn Sie den Microsoft DFÜ-Dialer benutzen, tragen Sie hier die Script-Datei unter Eingabe von Pfad und Namen ein.

(Siehe →Grundeinstellungen, Micosoft DFÜ-Dialer verwenden)

5.1.3 HTTP-Anmeldung



Mit den Einstellungen in diesem Parameterfeld kann die automatische HTTP-Anmeldung vorgenommen werden. Zentral erstellte Anmelde-Skripts und die hinterlegten Anmeldedaten können vom Access Point (HotSpot) übernommen werden, ohne dass ein Browserfenster geöffnet wird.



Bitte beachten Sie, dass die Verbindung über einen HotSpot-Betreiber gebührenpflichtig ist. Sie müssen den Geschäftsbedingungen des HotSpot-Betreibers zustimmen, wenn die Verbindung aufgebaut werden soll.

Parameter:

- ☐ Benutzername | HTTP-Anmeldung
- ☐ Passwort | HTTP-Anmeldung
- ☐ Passwort speichern | HTTP-Anmeldung
- ☐ HTTP Authentisierungs-Script | HTTP-Anmeldung

Mit diesen Daten wird die Anmeldung am HotSpot automatisiert. Dies geschieht in der Weise, dass bei einem Verbindungsaufbau zum Access Point von dort ein HTTP Redirect an den Client mit einer Website zur Anmeldung erfolgt. Anstatt eines Browser-Starts zur HTTP-Authentisierung, erfolgt mit den hier gemachten Eingaben die Authentisierung automatisch im Hintergrund.

Für die script-gesteuerte Anmeldung kann ein Script aus dem Installationsverzeichnis `<install>\scripts\samples` für weitere HotSpots entsprechend angepasst werden.



Bei der Verbindungsart WLAN werden die Authentisierungsdaten für den Hotspot aus den WLAN-Einstellungen übernommen, bzw. wenn diese deaktiviert sind, aus dem Management Tool der WLAN-Karte.

■ **Benutzername | HTTP-Anmeldung**

Dies ist der Benutzername, den Sie von Ihrem HotSpot-Betreiber erhalten haben.

■ **Passwort | HTTP-Anmeldung**

Dies ist das Passwort, das Sie von Ihrem HotSpot-Betreiber erhalten haben. Das Passwort wird mit verdeckter Schreibweise (mit *) eingegeben.

■ **Passwort speichern | HTTP-Anmeldung**

Nachdem das Passwort eingegeben wurde, kann es gespeichert werden

■ **HTTP Authentisierungs-Script | HTTP-Anmeldung**

Hier kann nach Klick auf den Suchen-Button [...] das hinterlegte Anmelde-Script selektiert werden.

Um eingehende Zertifikate bei der HTTP-Authentisierung überprüfen zu können, muss im Script die Variable CACERTDIR gesetzt worden sein. Desweiteren können auch Inhalte des WEB Server-Zertifikats überprüft werden. Hierzu stehen weitere Variablen zur Verfügung:

CACERTVERIFY_SUBJECT

überprüft den Inhalt des Subjects (z.B. cn=WEB Server 1)

CACERTVERIFY_ISSUER

Überprüft den Inhalt der Issuers

CACERTVERIFY_FINGERPRINT

überprüft den MD5 Fingerprint des Aussteller-Zertifiats

Stimmt der Inhalt der Variable mit dem eingegebenen Zertifikat nicht überein, wird die SSL-Verbindung nicht hergestellt und eine Log-Meldung im Monitor ausgegeben.

5.1.4 Modem



Dieses Parameterfeld erscheint ausschließlich, wenn Sie als “Verbindungsmedium” “Modem” gewählt haben. Alle nötigen Parameter zu dieser Verbindungsart sind hier gesammelt.

Parameter:

- ☐ Modem
- ☐ Anschluss
- ☐ Baudrate
- ☐ Com Port freigeben
- ☐ Modem Init. String
- ☐ Dial Prefix
- ☐ APN
- ☐ SIM PIN

■ Modem

Dieses Parameterfeld zeigt die auf dem PC installierten Modems. Wählen Sie aus der Liste das gewünschte Modem aus.

Je nachdem, welches Modem Sie wählen, werden die zugehörigen Parameter "Com Port" und "Modem Init. String" automatisch in die Konfigurationsfelder des Telefonbuchs aus der Treiberdatenbank des Systems übernommen.

(Weitere Parameter für dieses Kommunikationsmedium können auch über die Systemsteuerung des PCs konfiguriert werden.)



Hinweis: Bitte beachten Sie, dass Sie das Modem vor der Konfiguration der Verbindung im Telefonbuch installiert haben müssen, um es korrekt für Kommunikationsverbindungen nutzen zu können.

■ Anschluss

An dieser Stelle bestimmen Sie, welcher Com Port von Ihrem Modem genutzt werden soll. Wenn Sie bereits Modems unter Windows installiert haben, wird der während dieser Installation festgesetzte Com Port automatisch übernommen, sobald Sie das entsprechende Gerät unter "Modem" auswählen.



Hinweis: Wenn Sie ein bereits unter Ihrem System installiertes Modem nutzen möchten, so wählen Sie vor der Einstellung des Com Ports zuerst das gewünschte Gerät unter "Modem" aus – der entsprechend konfigurierte Com Port wird dann automatisch gesetzt.

■ Baudrate

Die Baudrate beschreibt die Übertragungsgeschwindigkeit zwischen Com Port und Modem. Wenn Ihr Modem z.B. mit 14.4 Kbits übertragen kann, sollten sie die nächsthöhere Baudrate 19200 wählen.

Folgende Baudraten können gewählt werden:
1200, 2400, 4800, 9600, 19200, 38400, 57600 und 115200

■ Com Port freigeben

Wenn Sie für Ihren Client ein analoges Modem verwenden, kann es wünschenswert sein, dass der Com Port nach Beendigung der Kommunikation für andere Applikationen freigegeben wird (z.B. Fax). In diesem Fall stellen Sie den Parameter auf "Ein". Solange der Parameter in der Standardstellung auf "Aus" bleibt, wird der Com Port ausschließlich von der Client Software genutzt.

■ Modem Init. String

Je nach eingesetztem Handy oder Modem und der jeweiligen Verbindungsart können AT-Kommandos nötig sein. In diesem Fall müssen die jeweiligen Kommandos dem zugehörigen Benutzerhandbuch oder den Mitteilungen der Telefongesellschaft bzw. des Providers entnommen werden. Jedes der in diesem Fall einzutragenden Kommandos muss mit einem <cr> (Carriage Return) abgeschlossen werden.

■ Dial Prefix

Dieses Feld ist optional. Ist das Modem korrekt installiert und steht der Software als Standardtreiber zur Verfügung, so muss hier kein Eintrag vorgenommen werden. Der Dial Prefix ist nur in seltenen Ausnahmefällen nötig. Ziehen Sie dazu das Modem-Handbuch zu Rate.

Im folgenden einige Beispiele für Dial Prefix:

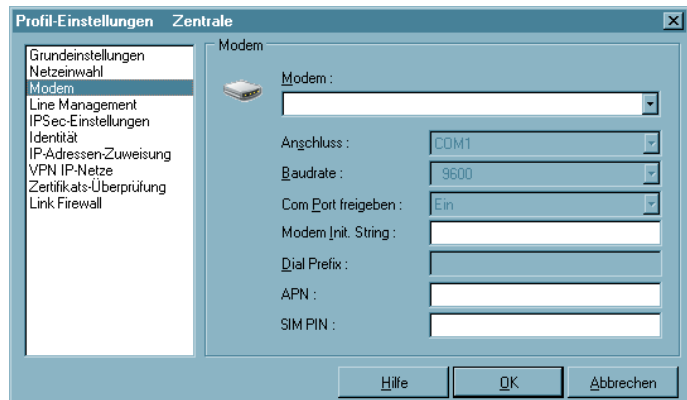
ATDT
ATDP
ATDI
ATDX

■ APN

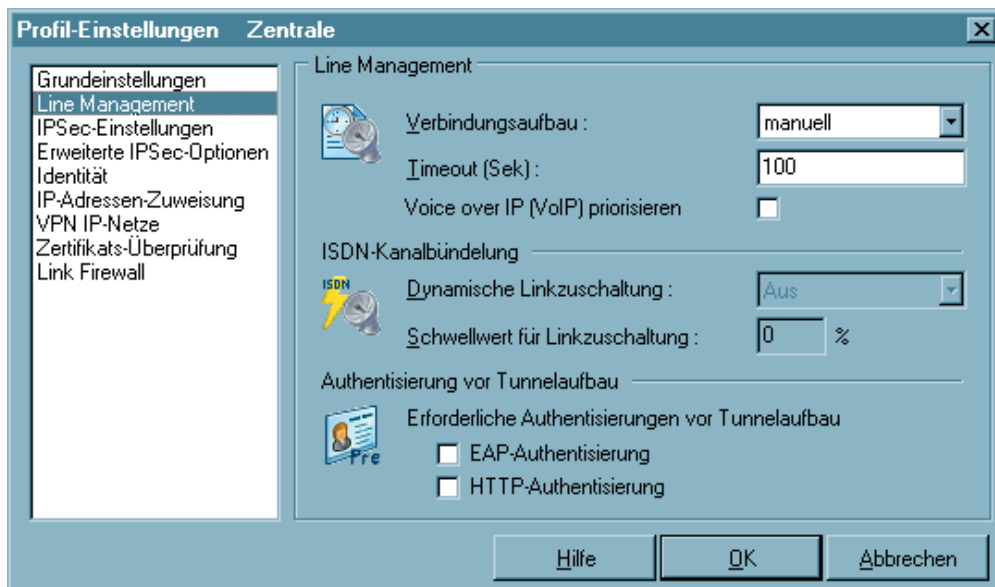
Der APN (Access Point Name) wird für die GPRS- und UMTS-Einwahl benötigt. Sie erhalten ihn von Ihrem Provider. Der APN wird insbesondere zu administrativen Zwecken genutzt.

■ SIM PIN

Benutzen Sie eine SIM-Einsteckkarte für GPRS oder UMTS, so geben Sie hier die PIN für diese Karte ein. Benutzen Sie ein Handy, so muss diese PIN am Mobiltelefon eingegeben werden.



5.1.5 Line Management



In diesem Parameterfeld bestimmen Sie, wie der “Verbindungsaufbau” erfolgen soll und stellen die Timeout-Werte ein.

Wenn der Client das Verbindungsmedium “ISDN” nutzt, können Sie in diesem Parameterfeld auch eine Kanalbündelung aktivieren. Bitte beachten Sie dabei, dass die Kanalbündelung nur funktionieren kann, wenn sowohl der Client als auch der NAS für eine Verbindung über gleich viele mögliche Kanäle verfügen.

Welche Authentisierung vor dem Tunnelaufbau erforderlich ist, wird vom Zielnetzwerk oder vom HotSpot-Betreiber vorgegeben.

Parameter:

- ☐ Verbindungsaufbau
- ☐ Timeout
- ☐ Voice over IP (VoIP) priorisieren
- ☐ Dynamische Linkzuschaltung
- ☐ Schwellwert für Linkzuschaltung
- ☐ EAP-Authentisierung
- ☐ HTTP-Authentisierung

■ Verbindungsaufbau

Hier definieren Sie, wie die Verbindung zu einem, im Telefonbuch eingetragenen Zielsystem, aufgebaut werden soll. Drei Modi stehen zur Wahl:

automatisch	=	(default) Dies bedeutet, dass die Client Software die Verbindung zum Zielsystem automatisch herstellt. Das Trennen der Verbindung erfolgt je nach Protokoll Ihres Systems, entsprechend den Anforderungen der Anwendung und den Einstellungen im Telefonbuch.
manuell	=	In diesem Fall müssen Sie die Verbindung zum Zielsystem manuell herstellen. Ein Trennen der Verbindung erfolgt je nach eingestelltem Wert für den Timeout.
wechselnd	=	Wird dieser Modus gewählt, muss zunächst die Verbindung "manuell" aufgebaut werden. Danach wechselt der Modus je nach Verbindungsabbau: – Wird die Verbindung nun mit Timeout beendet, so wird die Verbindung bei der nächsten Anforderung "automatisch" hergestellt, – wird die Verbindung manuell abgebaut, muss sie auch wieder manuell aufgebaut werden.



Wichtig: Sollten Sie den Verbindungsaufbau auf "manuell" setzen, so sollten Sie den Timeout aktivieren, um den Verbindungsabbau zu automatisieren. Andernfalls könnten unnötige Verbindungskosten für Sie entstehen.

■ Timeout

Mit diesem Parameter wird der Zeitraum festgelegt, der nach der letzten Datenbewegung (Empfang oder Versenden) verstreichen muss, bevor automatisch ein Verbindungsabbau erfolgt. Der Wert wird in Sekunden zwischen 0 und 65535 angegeben. Der Standardwert ist "100".

Wenn Ihr Anschluss (ISDN oder analog) einen Gebührenimpuls erhält, verwendet die Client Software das Impulsintervall, um den optimalen Zeitpunkt des Verbindungsabbaus bezüglich dem von Ihnen gesetzten Wert zu ermitteln. Der nach Gebührentakt optimierte Timeout läuft im Hintergrund und hilft die Verbindungskosten zu reduzieren.



Hinweis: Um den Timeout zu aktivieren, ist es nötig, einen Wert zwischen 1 und 65535 einzutragen. Mit dem Wert "0" wird der automatische Timeout (Verbindungsabbau) nicht ausgeführt. Der Wert "0" bedeutet, dass das Trennen der Verbindung manuell durchgeführt werden muss. Ziehen Sie bei diesem Parameter bitte Ihren Internet Provider oder Ihren Systemadministrator zu Rate.



Wichtig: Der Timer für das gewählte Zeitintervall läuft erst dann an, wenn keine Datenbewegung oder Handshaking mehr auf der Leitung stattfindet.

■ Voice over IP (VoIP) priorisieren

Wird dieser Client für Kommunikation mit Voice over IP genutzt, so sollte diese Funktion aktiviert werden, um die Sprachdaten verzögerungs- und verzerrungsfrei senden und empfangen zu können.

■ Dynamische Linkzuschaltung (Nur für ISDN)

Mit dynamischer Linkzuschaltung (für ISDN) kann die Client Software bis zu 8 ISDN B-Kanäle bündeln. Um diese Funktion in vollem Umfang nutzen zu können, muss allerdings Ihr PC wie auch das Zielsystem mit der nötigen Anzahl von So-Schnittstellen (4) ausgestattet sein.

Die dynamische Linkzuschaltung funktioniert nur, wenn sie auch vom Network Access Server des Zielsystems unterstützt wird. Mit dynamischer Linkzuschaltung erhöhen sich zwar die Kosten für jeden zugeschalteten B-Kanal, gleichzeitig verringern sie sich jedoch in gleichem Maße, weil sich die Übertragungsdauer entsprechend verkürzt!

Mit diesem Parameter bestimmen Sie, wie die Linkzuschaltung erfolgen soll. Drei Möglichkeiten stehen zur Auswahl:

Aus	(standard)
Tx	Links werden zugeschaltet, entsprechend der Bitrate abgehender Daten
Rx	Links werden zugeschaltet, entsprechend der Bitrate eingehender Daten
TxRx	Links werden sowohl nach der Bitrate sowohl eingehender als auch abgehender Daten zugeschaltet

■ Schwellwert für Linkzuschaltung (Nur für ISDN)

Der Wert dieses Parameters teilt der Client Software die Bitrate mit, ab der ein weiterer Link (Kanal) zugeschaltet werden soll. Der Wert entspricht Prozenten der maximalen Bitrate. Mögliche Werte sind von 1 bis 100 (Prozent). Standardwert ist "20". Diese Einstellung gilt für Sender und Empfänger.

Die Zuschaltung eines weiteren Links erfolgt 8 Sekunden nach dem Erreichen des eingestellten Schwellwerts.

Diese Einstellung kommt nur zum Tragen, wenn die Linkzuschaltung aktiviert wurde.

■ EAP-Authentisierung

Muss sich der Client mit EAP (Extensible Authentication Protocol) authentisieren, so muss diese Funktion aktiviert werden. Sie bewirkt, dass für dieses Zielsystem die EAP-Konfiguration im Monitor-Menü unter “EAP-Optionen” zum Einsatz kommt.



Bitte beachten Sie, dass die EAP-Konfiguration im Monitor-Menü für alle Zielsysteme gültig ist und aktiv geschaltet sein muss, wenn diese linkspezifische Einstellung wirksam sein soll.

EAP wird dann eingesetzt, wenn für das wireless LAN ein Access Point verwendet wird, der 802.1x-fähig ist und eine entsprechende Authentisierung verlangt. EAP kann aber auch dann eingesetzt werden, wenn der Client über einen Router auf ein anderes Netzsegment des Firmennetzes zugreifen möchte. Generell wird mit EAP verhindert, dass sich unberechtigte Benutzer über die Hardware-Schnittstelle in das LAN einklinken.



Nach Konfiguration des EAP muss eine Statusanzeige im grafischen Feld des Monitors erscheinen. Ist dies nicht der Fall, so muss die EAP-Konfiguration im Monitor-Menü aktiv geschaltet werden. Durch einen Doppelklick auf das EAP-Symbol kann das EAP zurückgesetzt werden. Anschließend erfolgt die EAP-Verhandlung erneut.

■ HTTP-Authentisierung

Für die automatische HTTP-Authentisierung am Access Point (HotSpot) muss diese Funktion aktiviert werden.

Damit wird ein weiteres Parameterfeld “HTTP-Anmeldung” im Telefonbuch zugeschaltet, in welches im folgenden die Authentisierungsdaten eingegeben werden können (siehe oben →HTTP-Anmeldung).



Bei einem Link mit der Verbindungsart WLAN wird die HTTP-Anmeldung im Telefonbuch nicht zugeschaltet! Statt dessen wird mit der Aktivierung dieser Funktion bewirkt, dass für dieses Zielsystem die Authentisierungsdaten aus den WLAN-Einstellungen im Monitor-Menü zum Einsatz kommen.

5.1.6 IPSec-Einstellungen

Profil-Einstellungen Zentrale

Grundeinstellungen
Line Management
IPSec-Einstellungen
Erweiterte IPSec-Optionen
Identität
IP-Adressen-Zuweisung
VPN IP-Netze
Zertifikats-Überprüfung
Link Firewall

IPSec-Einstellungen

Gateway : 0.0.0.0

Richtlinien

IKE-Richtlinie : Automatischer Modus

IPSec-Richtlinie : Automatischer Modus

Exch. mode : Main Mode

PFS-Gruppe : None

Gültigkeit ... Editor ...

Hilfe OK Abbrechen



In diesem Parameterfeld geben Sie die IP-Adresse des Gateways ein. Darüber hinaus legen Sie die Richtlinien fest, die für die IPSec-Verbindung in der Phase 1- und Phase 2-Verhandlung verwendet werden sollen. Sofern der automatische Modus genutzt wird, akzeptiert der Client die Richtlinien, wie sie vom Gateway der Gegenstelle vorgegeben werden. Soll der IPSec Client als Initiator der Verbindung eigene Richtlinien verwenden, so müssen diese mit dem Richtlinien-Editor konfiguriert werden. Die erweiterten Optionen können nach Abstimmung mit der Gegenstelle eingesetzt werden.

Parameter:

- | | |
|---|-------------------------------------|
| ☐ Gateway | ☐ Exch. Mode |
| ☐ IKE-Richtlinie | ☐ PFS-Gruppe |
| ☐ IPSec-Richtlinie | |
| ☐ Richtlinien-Gültigkeit | |
| ☐ Richtlinien-Editor | |

■ Gateway

Dies ist die IP-Adresse des IPSec Gateways, auch Tunnel-Endpunkt. Sie erhalten die Adresse von Ihrem Administrator entweder als Hex-Adresse, wenn das Gateway über eine feste offizielle IP-Adresse verfügt – oder als Namens-String, wenn das Gateway eine wechselnde IP-Adresse von einem Internet Service Provider erhält.

Hex-Adresse: Die Adresse ist 32 Bits lang und besteht aus vier voneinander durch Punkte getrennte Zahlen.

Namens-String: Sie tragen den Namen ein, den Sie von Ihrem Administrator erhalten haben. Es handelt sich dabei um den DNS-Namen des Gateways, der beim DynDNS Service Provider hinterlegt wurde.

Ein zweites Gateway kann in der gleichen Syntax nach dem ersten durch ein Semikolon getrennt eingetragen werden.

■ IKE-Richtlinie

Die IKE-Richtlinie wird aus der Listbox ausgewählt. In der Listbox werden alle IKE-Richtlinien aufgeführt, die Sie im Richtlinien-Editor unter der Verzweigung “IKE-Richtlinie” angelegt haben. Die Richtlinien erscheinen in der Box mit dem Namen, den Sie bei der Konfiguration vergeben haben.

Sie finden zwei vorkonfigurierte Richtlinien im Richtlinien-Editor unter “IKE-Richtlinie” als “Pre-shared Key” und “RSA-Signatur”. Inhalt und Name dieser Richtlinien können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu Authentisierung und Verschlüsselungsalgorithmus auf (siehe →IKE-Richtlinie (editieren)), d.h. eine Richtlinie besteht aus verschiedenen Vorschlägen. Funktional unterscheiden sich diese Richtlinien durch Verwendung eines statischen Schlüssels bzw. einer RSA-Signatur.



Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Automatischer Modus: In diesem Fall kann die Konfiguration der IKE-Richtlinie mit dem im Richtlinien-Editor entfallen. Die Richtlinie wird vom Gateway der Gegenstelle vorgegeben und vom Client akzeptiert.

Pre-shared Key: Diese vorkonfigurierte Richtlinie kann ohne PKI-Unterstützung genutzt werden. Beidseitig wird der gleiche “Statische Schlüssel” verwendet (siehe →Pre-shared Key verwenden, Shared Secret im Parameterfeld “Identität”).

RSA-Signatur: Diese vorkonfigurierte Richtlinie kann nur mit PKI-Unterstützung eingesetzt werden. Als zusätzliche, verstärkte Authentisierung ist der Einsatz der RSA-Signatur nur sinnvoll unter Verwendung einer Smart Card oder eines Soft-Zertifikats.

■ IPSec-Richtlinie

Die IPSec-Richtlinie wird aus der Listbox ausgewählt. In der Listbox werden alle IPSec-Richtlinien aufgeführt, die Sie mit dem Richtlinien-Editor angelegt haben. Die Richtlinien erscheinen in der Box mit dem Namen, den sie bei der Konfiguration vergeben haben.

Funktional unterscheiden sich zwei IPSec-Richtlinien nach dem IPSec-Sicherheitsprotokoll AH (Authentication Header) oder ESP (Encapsulating Security Payload). Da der IPSec-Modus mit AH-Sicherung für flexiblen Remote Access völlig ungeeignet ist, wird nur die IPSec-Richtlinie mit ESP-Protokoll, "ESP - 3DES - MD5", standardmäßig vorkonfiguriert mit der Software ausgeliefert.

Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu IPSec-Protokoll und Authentisierung auf (siehe →IPSec-Richtlinie (editieren)), d.h. eine Richtlinie besteht aus verschiedenen Vorschlägen.



Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Automatischer Modus: In diesem Fall kann die Konfiguration der IKE-Richtlinie mit dem Richtlinien-Editor entfallen.

ESP - 3DES - MD5 (oder anderer Name): Wenn Sie den Namen der vorkonfigurierten IPSec-Richtlinie wählen, muss die gleiche Richtlinie mit all ihren Vorschlägen für alle Benutzer gültig sein. Dies bedeutet, dass sowohl auf Client- als auch auf Server-Seite die gleichen Vorschläge für die Richtlinien zur Verfügung stehen müssen.

■ Exch. Mode

Der Exchange Mode (Austausch-Modus) bestimmt wie der Internet Key Exchange vonstatten gehen soll. Zwei unterschiedliche Modi stehen zur Verfügung, der Main Mode, auch Identity Protection Mode und der Aggressive Mode. Die Modi unterscheiden sich durch die Anzahl der Messages und durch deren Verschlüsselung.

Main Mode: Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden – daher auch Identity Protection Mode.

Aggressive Mode: Im Aggressive Mode gehen nur drei Meldungen über den Kontrollkanal, wobei nichts verschlüsselt wird.

■ PFS-Gruppe

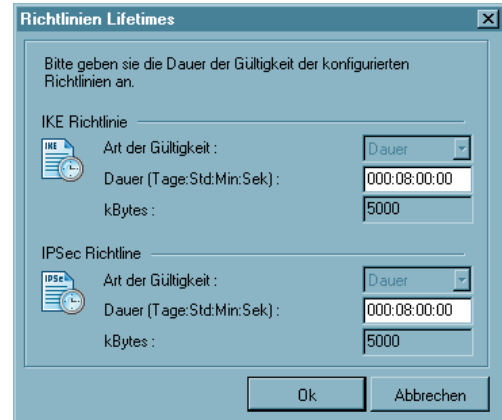
Mit Auswahl einer der angebotenen Diffie-Hellman-Gruppen wird festgelegt, ob ein kompletter Diffie-Hellman-Schlüsselaustausch (PFS, Perfect Forward Secrecy) in Phase 2 zusätzlich zur SA-Verhandlung stattfinden soll. Standard ist "keine".

Richtlinien-Gültigkeit

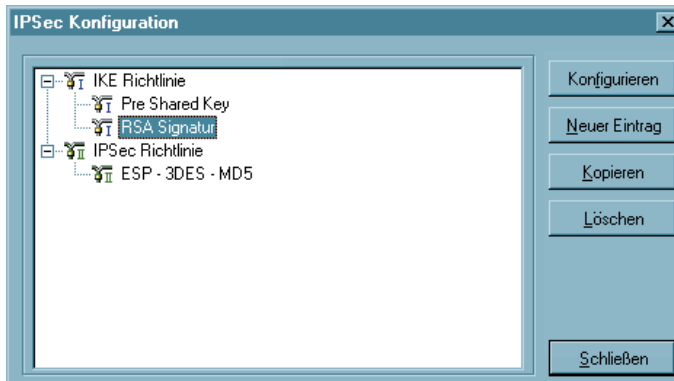
Die hier definierte Dauer der Gültigkeit gilt für alle Richtlinien gleichermaßen.

■ Dauer

Die Menge der kBytes oder die Größe der Zeitspanne kann eigens eingestellt werden.



Richtlinien-Editor



Zur Konfiguration der Richtlinien und gegebenenfalls einer statischen Secure Policy Database wird dieser Menüpunkt angeklickt. Damit öffnet sich ein Konfigurationsfenster mit der Verzweigung der Richtlinien und Secure Policy Database zu IPSec, sowie Buttons zur Bedienung auf der rechten Seite des Konfigurationsfensters.

Um die (Standard-)Werte der Richtlinien zu editieren, wählen Sie mit der Maus die Richtlinie, deren Werte Sie ändern möchten – die Buttons zur Bedienung werden dann aktiv.

Konfigurieren

Um eine Richtlinie oder eine SPD abzuändern, wählen Sie mit der Maus den Namen, der Gruppe deren Werte Sie ändern möchten und klicken auf “Konfigurieren”. Dann öffnet sich das entsprechende Parameterfeld mit den IPSec-Parametern.

Neuer Eintrag

Wenn Sie eine neue Richtlinie oder SPD anlegen möchten, selektieren Sie eine der Richtlinien oder die SPD und klicken auf “Neuer Eintrag”. Die neue Richtlinie oder SPD wird erzeugt. Alle Parameter sind auf Standardwerte gesetzt, bis auf den Namen.

Kopieren

Um die Parameter-Einstellungen eines bereits definierten Richtlinie oder SPD zu kopieren, markieren sie die zu kopierende Richtlinie oder SPD und klicken auf “Kopieren”. Daraufhin wird das Parameterfeld geöffnet. Ändern Sie nun den Namen und klicken Sie anschließend Ok. Die neue Richtlinie oder SPD ist nun angelegt. Die Parameterwerte sind zu denen der kopierten identisch, bis auf den Namen.



Löschen

Wenn Sie eine Richtlinie oder SPD aus dem Konfigurationsbaum löschen wollen, selektieren Sie sie und klicken auf “Löschen”. Die Richtlinie oder SPD ist damit auf Dauer aus der IPSec-Konfiguration gelöscht.

Schließen

Wenn Sie das IPSec-Feld schließen, kehren Sie zum Monitor zurück. Die Daten werden so wie sie konfiguriert wurden behalten.

IKE-Richtlinie (editieren)

Authentisierung	Verschlüsselung	Hash	DH-Gruppe
Preshared Key	AES 128 Bit	SHA	DH-Gruppe 2 (1024 Bit)

Authentisierung :

Verschlüsselung :

Hash :

DH-Gruppe :

Die Parameter in diesem Feld beziehen sich auf die Phase 1 des Internet Key Exchange (IKE) mit dem der Kontrollkanal für die SA-Verhandlung aufgebaut wird. Den IKE-Modus (Austausch-Modus / Exchange Mode), Main Mode oder Aggressive Mode, bestimmen Sie in dem Parameterfeld “IPSec-Einstellungen” im Telefonbuch. Die IKE-Richtlinien, die Sie hier konfigurieren, werden zur Auswahl gelistet.

Inhalt und Name dieser Richtlinien können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu Authentisierung und Verschlüsselungsalgorithmus auf, d.h. eine Richtlinie kann aus mehreren Vorschlägen bestehen.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Mit den Buttons “Hinzufügen” und “Entfernen” erweitern Sie die Liste der Vorschläge oder löschen einen Vorschlag aus der Liste der Richtlinie.

■ Name | IKE-Richtlinie

Geben Sie dieser Richtlinie einen Namen, über den sie später einer SPD zugeordnet werden kann.

■ Authentisierung | IKE-Richtlinie

Bevor der Kontrollkanal für die Phase 1-Verhandlung (IKE Security Association) aufgebaut werden kann, muss beidseitig eine Authentisierung stattgefunden haben.

Zur gegenseitigen Authentisierung wird der allen gemeinsame pre-shared Key (statischer Schlüssel) verwendet. Diesen Schlüssel definieren Sie im Parameterfeld "Identität".

■ Verschlüsselung | IKE-Richtlinie

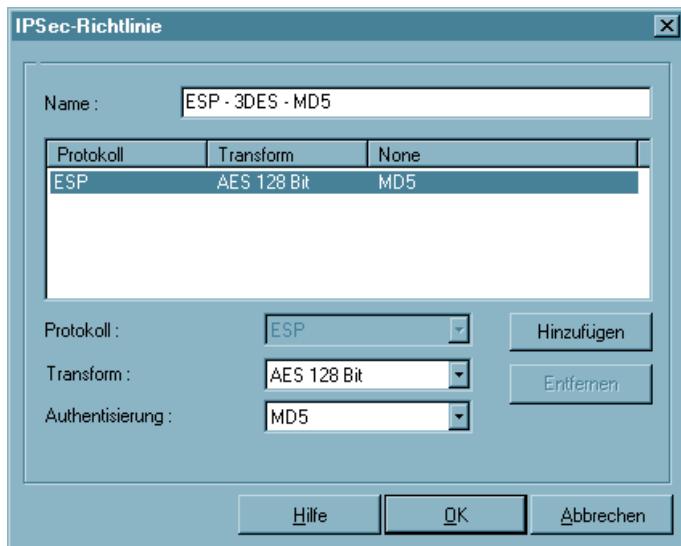
Nach einem der optionalen Verschlüsselungsalgorithmen erfolgt die symmetrische Verschlüsselung der Messages 5 und 6 im Kontrollkanal, sofern der Main Mode (Identity Protection Mode) gefahren wird. Zur Wahl stehen: DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

■ Hash | IKE-Richtlinie

Modus, wie der Hash-Wert über die ID bzw. das Zertifikat der Messages im Kontrollkanal gebildet wird. Zur Wahl stehen: MD5 (Message Digest, Version 5), SHA (Secure Hash Algorithm), SHA 256, SHA 384 und SHA 512 Bit

■ DH-Gruppe | IKE-Richtlinie

Mit der Wahl einer der angebotenen Diffie-Hellman-Gruppen wird festgelegt, wie sicher der Key Exchange im Kontrollkanal erfolgen soll, nach dem der spätere symmetrische Schlüssel erzeugt wird. Je höher die DH Group desto sicherer ist der Key Exchange.

IPSec-Richtlinie (editieren)


Die IPSec-Richtlinien (Phase-2-Parameter), die Sie hier konfigurieren, werden zur Auswahl für die SPD gelistet.



Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Mit den Buttons “Hinzufügen” und “Entfernen” erweitern Sie die Liste der Vorschläge oder löschen einen Vorschlag aus der Liste der Richtlinie.

■ Name | IPSec-Richtlinie

Geben Sie dieser Richtlinie einen Namen, über den Sie sie später einer SPD zuordnen können.

■ Protokoll | IPSec-Richtlinie

Der fest eingestellte Standardwert ist ESP.

■ Transformation (ESP) | IPSec-Richtlinie

Wenn das Sicherheitsprotokoll ESP eingestellt wurde, kann hier definiert werden wie mit ESP verschlüsselt werden soll. Zur Wahl stehen die gleichen Verschlüsselungsalgorithmen wie für Layer 2: DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

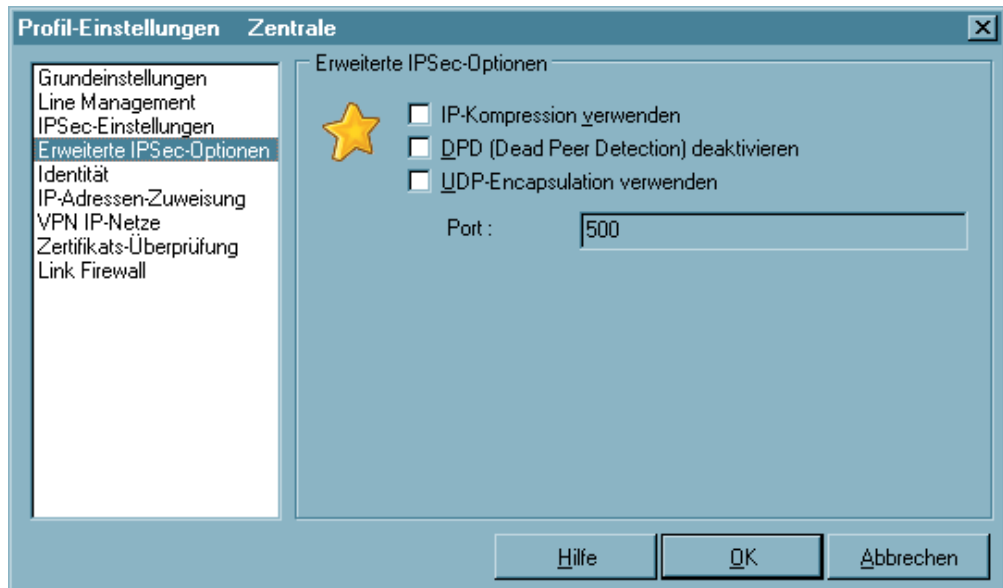
■ Transformation (Comp) | IPSec-Richtlinie

IPSec-Kompression. Die Datenübertragung mit IPSec kann ebenso komprimiert werden wie ein Transfer ohne IPSec. Dies ermöglicht eine Steigerung des Durchsatzes um maximal das 3-fache. Nach Selektion des Protokolls “Comp” (Kompression) kann zwischen LZS- und Deflate-Kompression gewählt werden.

■ Authentisierung | IPSec-Richtlinie

Für das Sicherheitsprotokoll ESP kann der Modus der Authentisierung eigens eingestellt werden. Zur Wahl stehen: MD5, SHA, SHA 256, SHA 384 und SHA 512 Bit.

5.1.7 Erweiterte IPSec-Optionen



In diesem Parameterfeld können weitere Einstellungen vorgenommen werden.

Parameter:

- ☐ IP-Kompression (LZS) verwenden
- ☐ DPD (Dead Peer Detection) deaktivieren
- ☐ UDP-Encapsulation verwenden

■ IP-Kompression (LZS) verwenden

Die Datenübertragung mit IPSec kann ebenso komprimiert werden wie ein Transfer ohne IPSec. Dies ermöglicht eine Steigerung des Durchsatzes um maximal das 3-fache.

■ DPD (Dead Peer Detection) deaktivieren

DPD (Dead Peer Detection) und NAT-T (NAT Traversal) werden automatisch im Hintergrund ausgeführt, sofern dies das Ziel-Gateway unterstützt. Der IPSec Client nutzt DPD, um in regelmäßigen Intervallen zu prüfen, ob die Gegenstelle noch aktive ist. Ist dies nicht der Fall erfolgt ein automatischer Verbindungsabbau.

Mit dieser Funktion kann DPD ausgeschaltet werden.

■ UDP-Encapsulation verwenden

Mit UDP-Encapsulation muss an der externen Firewall nur der Port 4500 freigeschaltet werden (anders bei NAT Traversal oder UDP 500 mit ESP). Das NCP Gateway erkennt die UDP-Encapsulation automatisch.

Wird die UDP-Encapsulation verwendet, so kann der Port frei gewählt werden. Standard für IPSec mit UDP ist der Port 4500, für IPSec ohne UDP der Port 500.

5.1.8 Identität

Profil-Einstellungen Zentrale

Identität

Lokale Identität

Typ : IP-Adresse

ID :

☒ Pre-shared Key verwenden

Shared Secret :

Bestätigung Secret :

☒ Extended Authentication (XAUTH) verwenden

Benutzername : ml

Passwort : **

Zugangsdaten aus Konfiguration verwenden

Hilfe OK Abbrechen



Entsprechend des Sicherheitsmodus IPsec können noch detailliertere Sicherheitseinstellungen vorgenommen werden.

Parameter:

- ☐ Typ | Identität
- ☐ ID | Identität
- ☐ Pre-shared Key verwenden
- ☐ Extended Authentication (XAUTH) verwenden
- ☐ Benutzername | Identität
- ☐ Passwort | Identität
- ☐ Zugangsdaten aus Konfiguration verwenden

■ Typ | Identität

Bei IPSec wird zwischen abgehenden und eingehenden Verbindungen unterschieden. Der Wert, den der Initiator als ID für eine abgehende Verbindung gewählt hat, muss bei der Gegenstelle als ID für eingehende Verbindungen gewählt sein.

Folgende ID-Typen stehen zur Auswahl:

- IP Address
- Fully Qualified Domain Name
- Fully Qualified Username
(entspricht der E-Mail-Adresse des Benutzers)
- IP Subnet Address
- ASN1 Distinguished Name
- ASN1 Group Name
- Free String used to identify Groups

■ ID | Identität

Bei IPSec wird zwischen abgehenden und eingehenden Verbindungen unterschieden. Der Wert, den der Initiator als ID für eine abgehende Verbindung gewählt hat, muss bei der Gegenstelle als ID für eingehende Verbindungen gewählt sein.

Entsprechend dem ID-Typ muss die zugehörige ID als String eingetragen werden.

■ Pre-shared Key verwenden

Der Pre-shared Key wird zur Verschlüsselung verwendet und ist ein String beliebiger Zeichen in einer maximalen Länge von 255 Zeichen. Alle alphanumerischen Zeichen können verwendet werden. Wenn die Gegenstelle einen Pre-shared Key während der IKE-Verhandlung erwartet, dann muss dieser Schlüssel in das Feld “Shared Secret” eingetragen werden. Bestätigen Sie das “Shared Secret” im darunter liegenden Feld. Der gleiche Pre-shared Key muss auf beiden Seiten verwendet werden.

Wird der Pre-shared Key nicht verwendet, so wird zur Verschlüsselung der Private Key eines zu konfigurierenden Zertifikats genutzt.

■ Extended Authentication (XAUTH) verwenden

Wird “IPSec-Tunneling” genutzt, so kann die Authentisierung über Extended Authentication (XAUTH Protokoll, Draft 6) erfolgen. Wird XAUTH eingesetzt und vom Gateway unterstützt, so aktivieren Sie “Benutze erweiterte Authentisierung (XAUTH)”. Zusätzlich zum pre-shared Key können dann noch folgende Parameter gesetzt werden:

Benutzername = Benutzername des IPSec-Benutzers

Passwort = Kennwort des IPSec-Benutzers

■ Benutzername | Identität

Den Benutzernamen für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.



Hinweis: Dieser Parameter wird nur benötigt, um Zugriff auf das Gateway der remote Seite zu bekommen.

■ Passwort | Identität

Das Passwort für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.



Hinweis: Dieser Parameter wird nur benötigt, um Zugriff auf das Gateway der remote Seite zu bekommen.

■ Zugangsdaten aus Konfiguration verwenden

Als Zugangsdaten für das VPN können folgende Einträge ausgelesen und verwendet werden:

Zugangsdaten aus Konfiguration verwenden:

Dies bedeutet, dass die in diesem Parameterfeld unter “Benutzername” und “Passwort” gemachten Angaben zur erweiterten Authentisierung verwendet werden.

Zugangsdaten aus Zertifikat (E-Mail) verwenden:

Dies bedeutet, dass statt “Benutzername” und “Passwort” der E-Mail-Eintrag des Zertifikats verwendet wird.

Zugangsdaten aus Zertifikat (Common Name) verwenden:

Dies bedeutet, dass statt “Benutzername” und “Passwort” der Benutzer-Eintrag des Zertifikats verwendet wird.

Zugangsdaten aus Zertifikat (Seriennummer) verwenden:

Dies bedeutet, dass statt “Benutzername” und “Passwort” die Seriennummer des Zertifikats verwendet wird.

5.1.9 IP-Adressen-Zuweisung



In diesem Parameterfenster wird eingestellt, wie die IP-Adressen vergeben werden sollen. Außerdem kann der durch die PPP-Verhandlung automatisch zugewiesene Server durch alternative Server ersetzt werden. Dazu muss in den Netzwerk-Einstellungen des Betriebssystems der DNS-Modus eingestellt sein.

Parameter:

- ☐ IKE Config Mode verwenden
- ☐ Lokale IP-Adresse verwenden
- ☐ IP-Adresse manuell vergeben
- ☐ DNS/WINS
- ☐ DNS-Server
- ☐ WINS-Server
- ☐ Domain Name

■ IKE Config Mode verwenden

IP-Adressen und DNS Server werden über das Protokoll IKE-Config Mode (Draft 2) zugewiesen. Für die NAS-Einwahl können alle bisherigen WAN-Schnittstellen verwendet werden.

Bei "IPSec-Tunneling" wird im Hintergrund automatisch DPD (Dead Peer Detection) und NAT-T (NAT Traversal) ausgeführt, falls dies von der Gegenstelle unterstützt wird. Mit DPD prüft der Client in bestimmten Abständen, ob die Gegenstelle noch aktiv ist. Bei inaktiver Gegenstelle erfolgt ein automatischer Verbindungsabbau. Der Einsatz von NAT Traversal erfolgt beim Client automatisch und ist immer nötig, wenn auf Seiten des Zielsystems ein Gerät mit Network Address Translation zum Einsatz kommt.

■ Lokale IP-Adresse verwenden

In diesem Fall wird die aktuell in den Netzwerkeinstellungen des PCs konfigurierte IP-Adresse (auch DHCP) für den IPSec Client genutzt.

■ IP-Adresse manuell vergeben

Dies ist die IP-Adresse und die Subnet-Maske, die hier frei eingegeben werden können. In diesem Fall wird die hier eingetragene Adresse genutzt, unabhängig von der Konfiguration in den Netzwerkeinstellungen.

■ DNS/WINS

Mit IKE Config Mode werden dynamisch IP-Adressen des Clients, des DNS- und WINS-Servers sowie der Domain Name zugewiesen.

Wird diese Funktion aktiviert, so kann alternativ zu dem DNS/WINS-Server, der automatisch während der PPP-Verhandlung zum NAS/ISP zugewiesen wird, ein anderer DNS/WINS Server bestimmt werden.

■ DNS-Server

Der zuerst eingetragene DNS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt.

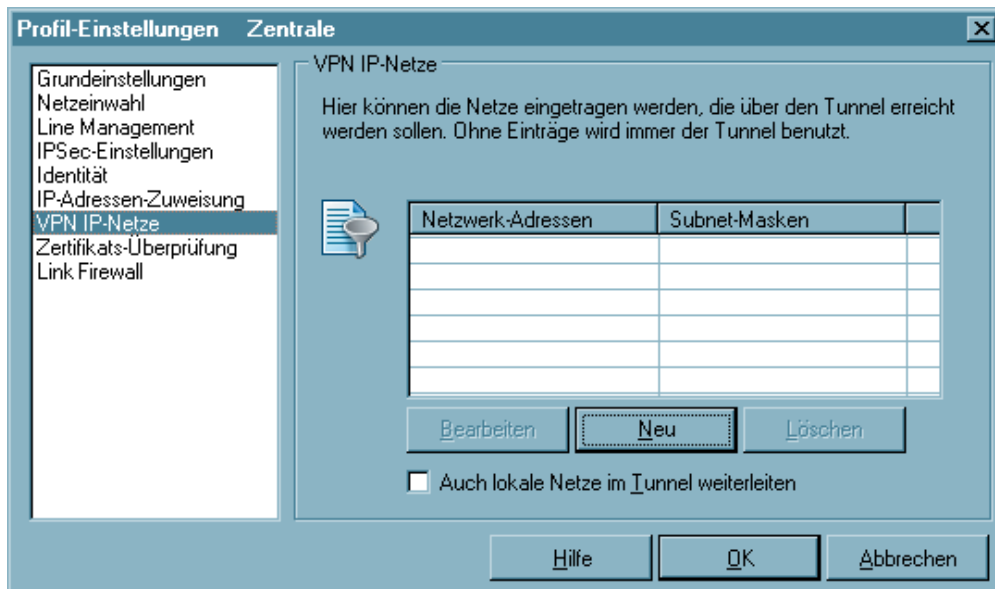
■ WINS-Server

Der zuerst eingetragene WINS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt.

■ Domain Name

Dies ist der Domain Name der sonst per DHCP dem System in den Netzwerkeinstellungen übergeben wird.

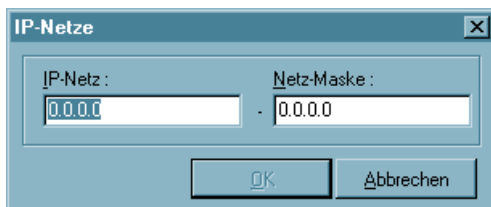
5.1.10 VPN IP-Netze



Hier können genau die IP-Netze definiert werden, über die der Client via VPN-Tunnel kommunizieren kann. Wenn Tunneling genutzt wird und hier keine Einträge erfolgen, so wird die Verbindung immer zum Tunnel-Endpunkt des Gateways aufgebaut. Soll alternierend einerseits ein Tunneling zur Zentrale erfolgen, andererseits über das Internet kommuniziert werden, so müssen hier die IP-Netze eingetragen werden, die vom Client erreicht werden sollen. Sie können dann zwischen dem Internet und dem Gateway der Firmenzentrale hin und her springen. Dies wird auch als "Split Tunneling" bezeichnet.

Parameter:

- ☐ Netzwerk-Adressen | VPN IP-Netze
- ☐ Subnet-Masken
- ☐ Auch lokale Netze im Tunnel weiterleiten



Klicken Sie auf den Button “Neu”, so können Sie in das daraufhin erscheinende Fenster (links) die IP-Adresse des Netzes und der Netzmaske eintragen.

■ Netzwerk-Adressen | VPN IP-Netze

In diesem Parameterfenster definieren Sie, in welchem IP-Netz oder welchen IP-Netzen der Client über VPN-Tunneling kommunizieren kann. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.



Bitte achten Sie ferner darauf, daß die IP-Adresse des Gateways nicht im Bereich der Netz-Adresse liegt.

■ Subnet-Masken

Hier tragen Sie die zugehörige Netzmaske des IP-Netzes ein. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

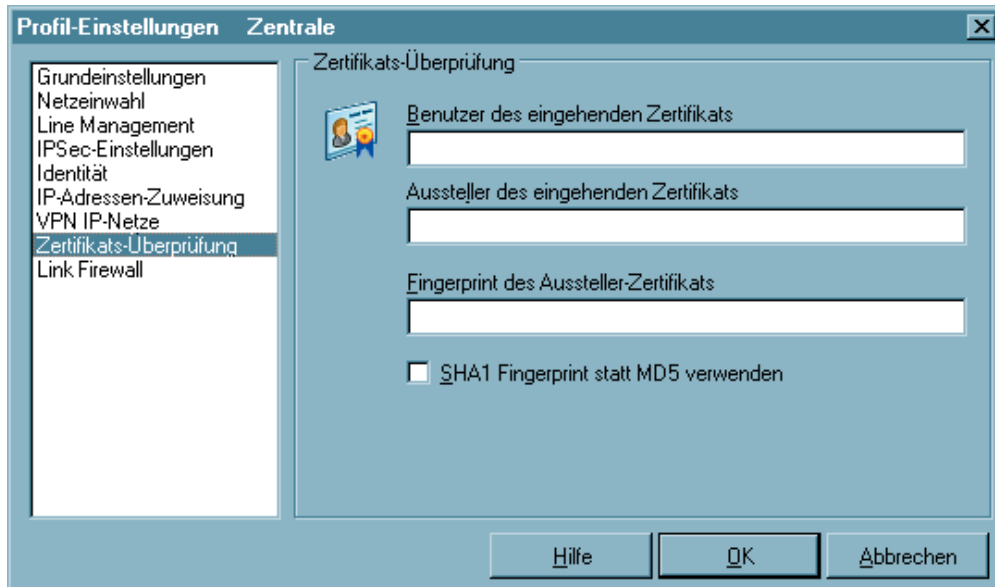


Bitte achten Sie darauf, daß die IP-Adresse des Gateways nicht im Bereich der Netz-Adresse liegt.

■ Auch lokale Netze im Tunnel weiterleiten

Wenn der Datenverkehr des lokalen Netzes über VPN-Tunneling weitergeleitet werden soll, so muss diese Funktion aktiviert werden.

5.1.11 Zertifikats-Überprüfung



Im Parameterfeld “Zertifikats-Überprüfung” kann pro Zielsystem des IPSec Clients vorgegeben werden, welche Einträge in einem Zertifikat der Gegenstelle (Gateway) vorhanden sein müssen (siehe –Eingehendes Zertifikat anzeigen, Allgemein).

Siehe auch:

- ☐ Benutzer des eingehenden Zertifikats
- ☐ Aussteller des eingehenden Zertifikats
- ☐ Fingerprint des Aussteller-Zertifikats
- ☐ SHA1 Fingerprint verwenden
- ☐ Weitere Zertifikats-Überprüfungen

■ Benutzer des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Benutzers, soweit bekannt – auch mit Wildcards -, verwendet werden. Vergleichen Sie dazu, welche Einträge bei “eingehendes Zertifikat anzeigen” unter Benutzer aufgeführt sind.

Verwenden Sie die Kürzel der Attributtypen. Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

```
cn      = Common Name / Name
s       = Surname / Nachname
g       = Givenname / Vorname
t       = Title / Titel
o       = Organisation / Firma
ou      = Organization Unit / Abteilung
c       = Country / Land
st      = State / Bundesland, Provinz
l       = Location / Stadt, Ort
email   = E-mail
```

Beispiel:

```
cn=VPNGW*, o=ABC, c=de
```

Der Common Name des Security Servers wird hier nur bis zur Wildcard “*” überprüft. Alle nachfolgenden Stellen können beliebig sein, etwa 1 - 5 als Numerierung. Die Organization Unit muss in diesem Fall immer ABC sein und das Land Deutschland.

■ Aussteller des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Ausstellers, soweit bekannt – auch mit Wildcards -, verwendet werden. Vergleichen Sie dazu welche Einträge bei “eingehendes Zertifikat anzeigen” unter Aussteller aufgeführt sind.

Verwenden Sie die Kürzel der Attributtypen. Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

```
cn      = Common Name / Name
s       = Surname / Nachname
g       = Givenname / Vorname
t       = Title / Titel
o       = Organisation / Firma
ou      = Organization Unit / Abteilung
c       = Country / Land
st      = State / Bundesland, Provinz
l       = Location / Stadt, Ort
email   = E-mail
```

Beispiel:

`cn=ABC GmbH`

Hier wird nur der Common Name des Ausstellers überprüft.

■ **Fingerprint des Aussteller-Zertifikats**

Um zu verhindern, dass ein Unberechtigter, der die vertrauenswürdige CA imitiert, ein gefälschtes Aussteller-Zertifikat verwenden kann, kann zusätzlich der Fingerprint des Ausstellers, soweit bekannt, eingegeben werden.

■ **SHA1 Fingerprint verwenden**

Der Algorithmus zur Erzeugung des Fingerprints kann MD5 (Message Digit 5) oder SHA1 (Secure Hash Algorithm 1) sein.

Weitere Zertifikats-Überprüfungen

Neben der Zertifikats-Überprüfung nach Inhalten erfolgt am IPSec Client eine weitere Zertifikatsprüfung in mehrfacher Hinsicht.

1. Auswahl der CA-Zertifikate

Der Administrator des Firmennetzes legt fest, welchen Ausstellern von Zertifikaten vertraut werden kann. Dies geschieht dadurch, dass er die CA-Zertifikate seiner Wahl in das Windows-Verzeichnis `\ncple\cacerts\` gespielt. Das Einspielen kann bei einer Software-Distribution mit Disketten automatisiert stattfinden, wenn sich die Aussteller-Zertifikate bei der Installation der Software im Root-Verzeichnis der ersten Diskette befinden. Nachträglich können Aussteller-Zertifikate automatisch über den Secure Update Server verteilt werden (siehe →Handbuch zum Update Server), oder – sofern der Benutzer über die notwendigen Schreibrechte in genanntem Verzeichnis verfügt – von diesem selbst eingestellt werden (siehe →CA-Zertifikate anzeigen).

Derzeit werden die Formate *.pem und *.crt für Aussteller-Zertifikate unterstützt. Sie können im Monitor unter dem Hauptmenüpunkt “Verbindung, Zertifikate, CA-Zertifikate anzeigen” eingesehen werden.

Wird am IPSec Client das Zertifikat einer Gegenstelle empfangen, so ermittelt der Client den Aussteller und sucht anschließend das Aussteller-Zertifikat, zunächst auf Smart Card oder PKCS#12-Datei, anschließend im Verzeichnis `NCPLE\CACERTS\`. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande.

Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen.

2. Überprüfung der Zertifikats-Erweiterung

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zertifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

Für den IPSec Client und das Gateway sind drei Erweiterungen von Bedeutung:

- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier

extendedKeyUsage:

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der IPSec Client, ob der definierte erweiterte Verwendungszweck "SSL-Server-Authentisierung" enthalten ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck "SSL-Server-Authentisierung" beinhalten muss. Dies gilt auch bei einem Rückruf an den Client über VPN.

subjectKeyIdentifier / authorityKeyIdentifier:

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann keine Übereinstimmung erkannt werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades.

(Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.)

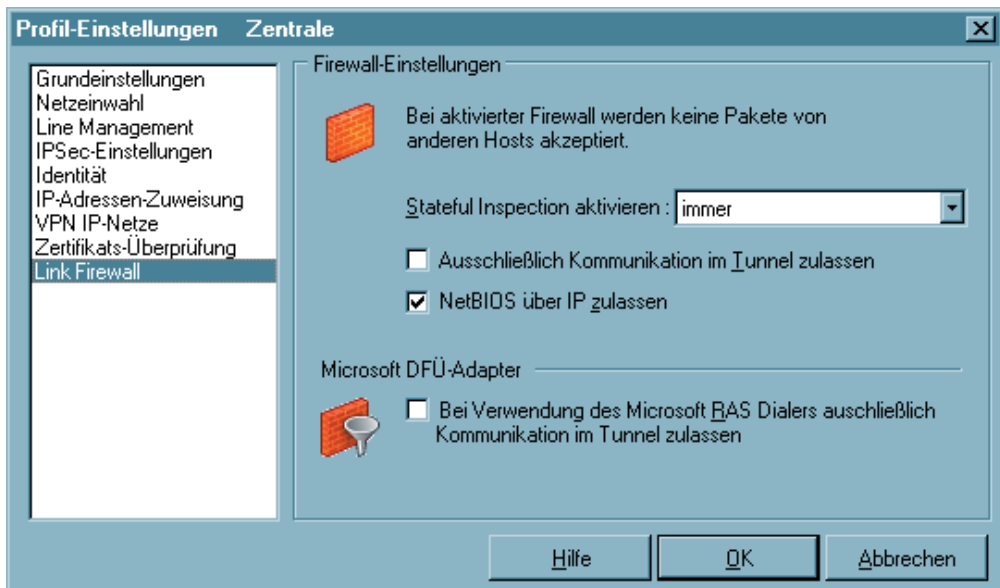
3. Überprüfung von Sperrlisten

Zu jedem Aussteller-Zertifikat kann dem IPSec Client die zugehörige CRL (Certificate Revocation List) zur Verfügung gestellt werden. Sie wird in das Windows-Verzeichnis \ncple\crls\ gespielt. Ist eine CRL vorhanden, so überprüft der IPSec Client eingehende Zertifikate daraufhin, ob sie in der CRL geführt sind. Gleiches gilt für eine ARL (Authority Revocation List), die in das Windows-Verzeichnis \ncple\arls\ gespielt werden muss.

Sind eingehende Zertifikate in den Listen von CRL oder ARL enthalten, wird die Verbindung nicht zugelassen.

Sind CRLs oder ARLs nicht vorhanden findet keine diesbezügliche Überprüfung statt.

5.1.12 Link Firewall



Die Link Firewall kann für alle Netzwerkadapter wie auch für RAS-Verbindungen genutzt werden. Die aktivierte Firewall wird in der grafischen Oberfläche des Clients als Symbol (Mauer mit Pfeil) dargestellt. Grundsätzliche Aufgabe einer Firewall ist es, zu verhindern, dass sich Gefahren aus anderen bzw. externen Netzen (Internet) in das eigene Netzwerk ausbreiten. Deshalb wird eine Firewall auch am Übergang zwischen Firmennetz und Internet installiert. Sie prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis vorher festgelegter Konfigurationen, ob ein Datenpaket durchgelassen wird oder nicht. Die hier zu aktivierende Firewall arbeitet nach dem Prinzip der Stateful Inspection. Stateful Inspection ist eine neue Firewall-Technologie und bietet den derzeit höchstmöglichen Sicherheitsstandard für Internet-Verbindungen und somit das Firmennetz. Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen verhindert diese Funktionalität den unbefugten Zugriff auf Daten und Ressourcen im zentralen Datennetz. Zum anderen überwacht sie als Kontrollinstanz den jeweiligen Status aller bestehenden Internet-Verbindungen. Die Stateful Inspection Firewall erkennt darüber hinaus, ob eine Verbindung "Tochterverbindungen" geöffnet hat – wie beispielsweise bei FTP oder Netmeeting – deren Pakete ebenfalls weitergeleitet werden müssen. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf (siehe →Handbuch, Beispiele und Erklärungen).

Parameter:

- | | |
|--|---|
| ☐ Stateful Inspection aktivieren | ☐ Bei Verwendung des Microsoft DFÜ-Dialers ausschließlich Kommunikation im Tunnel zulassen |
| ☐ Ausschließlich Kommunikation im Tunnel zulassen | |
| ☐ NetBIOS über IP zulassen | |

■ **Stateful Inspection aktivieren**

aus: Die Sicherheitsmechanismen der Firewall werden nicht in Anspruch genommen.

immer: Die Sicherheitsmechanismen der Firewall werden immer in Anspruch genommen, d.h. auch wenn keine Verbindung aufgebaut ist, ist der PC vor unberechtigten Zugriffen geschützt.

bei bestehender Verbindung: Der PC ist dann nicht angreifbar, wenn eine Verbindung besteht.

■ **Ausschließlich Kommunikation im Tunnel zulassen**

Ausschließlich Kommunikation im Tunnel zulassen: Bei aktivierter Firewall kann diese Funktion zusätzlich eingeschaltet werden, um in ein- und ausgehender Richtung ausschließlich VPN-Verbindungen zuzulassen.

■ **NetBIOS über IP zulassen**

Mit diesem Parameter wird ein Filter aufgehoben, der Microsoft NetBios Frames unterdrückt. Diesen Filter aufzuheben, um den Verkehr von NetBios Frames zu gestatten, ist immer dann zweckmäßig, wenn Sie zum Beispiel Microsoft Networking über den IP-Sec Client nutzen.

In der Standardeinstellung ist dieser Filter gesetzt, das heißt der Checkbutton nicht mit einem Haken markiert, so dass Microsoft NetBios Frames unterdrückt werden, damit sie den Datenverkehr nicht unnötig belasten. Markieren Sie den Checkbutton mit einem Haken, werden NetBios Frames over IP erlaubt.

■ **Bei Verwendung des Microsoft DFÜ-Dialers ausschließlich Kommunikation im Tunnel zulassen**

Bei Verwendung des Client-Monitors wird bei Aktivierung dieser Funktion verhindert, dass eine Kommunikation über den DFÜ-Dialer zum Internet stattfinden kann.

6. Verbindungsaufbau

■ Verbindungsaufbau zum Zielsystem

Sobald die Software installiert und ein Profil korrekt konfiguriert wurden, kann die Auswahl über das Profil an das Zielsystem stattfinden. Dabei ist auch die Art der Auswahl Bestandteil der Konfiguration eines Profils. Sie können aus drei Auswahl-Modi für den Verbindungsaufbau wählen: automatisch, manuell und wechselnd. Sie definieren den Modus des Verbindungsaufbaus zu einem Zielsystem in der Profil-Einstellungen unter "Verbindungsaufbau" im Parameterfeld "Line Management".

Automatischer Verbindungsaufbau:

Im Unterschied zu Microsoft RAS, bei dem jedes Ziel manuell ausgewählt werden muss, arbeitet die Client Software nach dem Prinzip der LAN-Emulation. Dabei ist es lediglich erforderlich, die entsprechende Applikations-Software zu starten (Email, Internet Browser, Terminal Emulation, etc.). Die Verbindung wird dann, entsprechend den Parametern des Zielsystems, automatisch aufgebaut und gehalten.

Manueller Verbindungsaufbau:

Daneben ist es auch möglich manuell die Verbindung zu einem ausgewählten Ziel herzustellen, indem Sie im Monitor "Verbindung" anklicken und "Verbinden" wählen.

Wechselnder Verbindungsaufbau:

Wird dieser Modus gewählt, muss zunächst die Verbindung "manuell" aufgebaut werden. Danach wechselt der Modus je nach Verbindungsabbau wie folgt:

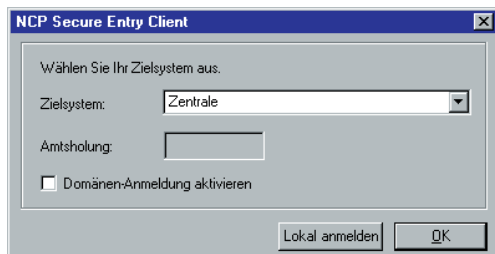
- Wird die Verbindung mit Timeout beendet, so wird die Verbindung bei der nächsten Anforderung "automatisch" hergestellt,
- wird die Verbindung "manuell" abgebaut, muss sie auch wieder "manuell" aufgebaut werden.

■ Verbinden

Gleich wie die Verbindung aufgebaut wird, der Monitor, sofern er im Vordergrund sichtbar ist, zeigt immer den Status des Verbindungsaufbaus wie in Abschnitt 3.1.6 "Symbole des Verbindungsaufbaus" beschrieben.

Client Logon

Erfolgt das Client Logon am Network Access Server vor dem Windows Logon an der remote Domäne, indem die Logon Optionen genutzt werden (siehe → Monitor, Logon Optionen), so erfolgt der Verbindungsaufbau prinzipiell genau so, wie oben unter “Verbinden” beschrieben.



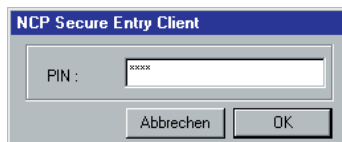
Nach der Auswahl des Zielsystems wird mit Klick auf den OK-Button der Verbindungsaufbau eingeleitet.

Lokal anmelden:

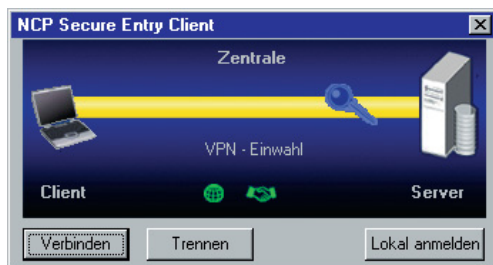
Ein Klick auf diesen Button bricht den Dialog zum Verbindungsaufbau ab.

Domänen-Anmeldung aktivieren:

Mit dieser Option ist eine sichere WAN-Domänen-Anmeldung möglich, auch wenn vorher keine ordnungsgemäße Abmeldung erfolgte. Die Anmeldung dauert einige Sekunden. Diese Funktion wird nicht benötigt, wenn bei einem ordnungsgemäßen Herunterfahren (Shut Down) des Computers eventuell gemappte Laufwerke korrekt getrennt wurden. (Diese Option ist nur bei einem NT-Server als Gegenstelle einsetzbar.)



Wurde die Verwendung eines (Soft-)Zertifikats konfiguriert, so muss zunächst die PIN eingegeben werden.



Die weiteren Stationen des Verbindungsaufbaus erfolgen genau so, wie oben unter “Verbinden” beschrieben ...



... bis die Verbindung steht.

■ Passwörter und Benutzernamen

Das Passwort (siehe → Netzeinwahl, Passwort) benötigen Sie, um sich gegenüber dem Network Access Server (NAS) ausweisen zu können, wenn die Verbindung aufgebaut ist. Das Passwort darf bis zu 254 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Passwort vom Zielsystem zugewiesen, da Sie vom Zielsystem auch erkannt werden müssen. Sie erhalten es von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator. Wenn Sie das Passwort eingeben, werden alle Zeichen als Stern (*) dargestellt, um sie vor ungewünschten Beobachtern zu verbergen. Es ist wichtig, dass Sie das Passwort genau nach der Vorgabe eintragen und dabei auch auf Groß- und Kleinschreibung achten.



Auch wenn Sie für den Verbindungsaufbau “automatisch” gewählt haben (siehe → Verbindungsaufbau zum Zielsystem), müssen Sie die Verbindung beim ersten Mal manuell aufbauen und das Passwort eingeben. Für jeden weiteren automatischen Verbindungsaufbau wird das Passwort selbständig übernommen, bis der PC erneut gebootet oder das Zielsystem gewechselt wird. D.h. für eine Reihe von “automatischen” Verbindungsaufbaus wird das Passwort nach der ersten Eingabe und dem ersten Verbindungsaufbau selbständig übernommen, auch wenn die Funktion “Passwort speichern” (siehe → Netzeinwahl) nicht aktiviert wurde. Erst ein Boot-Vorgang löscht das einmal eingegebene Passwort. (Beachten Sie dazu auch → Logon Optionen).



Soll das Passwort mit dem Booten nicht gelöscht werden, so muss die Funktion “Passwort speichern” aktiviert werden (siehe → Netzeinwahl). Bitte beachten Sie dabei, dass im Falle gespeicherter Passwörter, jedermann mit Ihrer Client Software arbeiten kann – auch wenn er die Passwörter nicht kennt.

Passwort für NAS-Einwahl

Wird das Passwort für die NAS-Einwahl nicht eingegeben oder nicht gespeichert, so wird es bei einem Verbindungsaufbau in einem eigenen Dialog abgefragt.

Der “Benutzername” für die Netzeinwahl muss immer in der Konfiguration für das Ziel eingegeben werden. Ohne ihn kann keine Einwahl an den NAS erfolgen. (Siehe → Profil-Einstellungen, Netzeinwahl)

Benutzername und Passwort für Extended Authentication

The screenshot shows the 'Profil-Einstellungen' window with the 'Zentrale' tab selected. On the left is a tree view with the following items: Grundeinstellungen, Netzeinwahl, Line Management, IPSec-Einstellungen, **Identität**, IP-Adressen-Zuweisung, VPN IP-Netze, Zertifikats-Überprüfung, and Firewall-Einstellungen. The 'Identität' section is active, showing 'Lokale Identität' with a 'Typ' dropdown set to 'IP-Adresse' and an empty 'ID' field. Below this are two sections: 'Pre-shared Key verwenden' (unchecked) with 'Shared Secret' and 'Bestätigung Secret' fields, and 'Extended Authentication (XAUTH) verwenden' (checked) with 'Benutzername' (ml) and 'Passwort' (xx) fields. At the bottom of the XAUTH section is a dropdown menu set to 'Zugangsdaten aus Konfiguration verwenden'. At the very bottom are 'Hilfe', 'OK', and 'Abbrechen' buttons.

Wird Extended Authentication eingesetzt, so müssen Benutzername und Passwort in der Konfiguration des Profils eingegeben werden, sonst findet kein Verbindungsaufbau statt (siehe → Profil-Einstellungen, Identität, Extended Authentication (XAUTH) verwenden).

■ Verbindungsabbruch und Fehler



Ereignet sich ein Fehler, so wird die Verbindung nicht hergestellt und die Fehlerursache im Monitor angezeigt (beachten Sie dazu den Abschnitt “Fehler- und ISDN-Meldungen”).



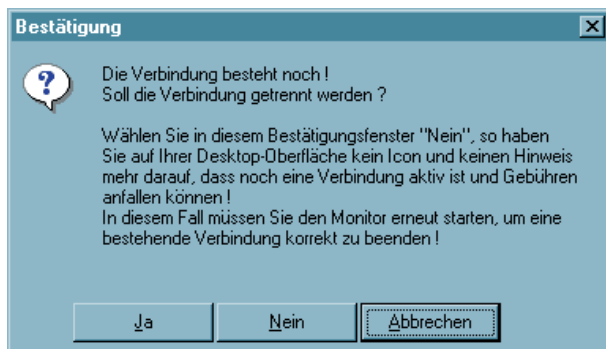
■ Trennen

Mit der Funktion “Trennen” wird der Abbau der aktuell bestehenden Verbindung manuell durchgeführt. Wenn Sie die Möglichkeit behalten wollen, jederzeit die Verbindung manuell abbauen zu können, setzen Sie den Verbindungsaufbau auf “manuell” und deaktivieren den automatischen Timeout, indem Sie ihn auf Null (0) setzen (→ Verbindungsaufbau).

Wenn die Verbindung abgebaut wird, wechselt die farbliche Darstellung der Verbindungslinie bis sie verschwindet und die Ampellampen des Monitors für die gesamte Offline-Dauer von grün zu rot.

■ Trennen und Beenden des Monitors

Besteht eine Verbindung noch, und wird der Monitor beendet, so wird nicht automatisch die Verbindung getrennt. Soll die möglicherweise kostenpflichtige Verbindung bestehen bleiben, obwohl der Monitor beendet wird, so wird dazu ausdrücklich eine Bestätigung von der Software verlangt (siehe Bild unten).



Klicken Sie in diesem Bestätigungsfenster auf "Nein", so haben Sie auf Ihrer Desktop-Oberfläche kein Icon und keinen Hinweis mehr darauf, dass noch eine Verbindung aktiv ist und Gebühren anfallen können! In diesem Fall müssen Sie den Monitor erneut starten, um eine bestehende Verbindung korrekt zu beenden!

7. Beispiele und Erklärungen

In diesem Abschnitt des Handbuchs werden einige Grundbegriffe des Routings und des IPSec-Verkehrs erklärt. Anhand von Beispielen wird die Konfiguration des IPSec Clients für bestimmte Funktionalitäten dargestellt.

7.1 IP-Funktionen

Um ein IP-Netzwerk korrekt zu konfigurieren, müssen die Regeln der IP-Adressierung eingehalten werden. Untenstehend sind einige Richtlinien und Terminologien aufgeführt. Zu weiteren Informationen über IP-Netzwerke wird entsprechende Fachliteratur empfohlen.

7.1.1 Geräte eines IP-Netzwerks

IP-Adressen werden den Schnittstellen der Geräte eines IP-Netzwerks zugewiesen. Diese Geräte werden auch als Hosts oder Rechner bezeichnet. Mehrfach vernetzten Geräten (z.B. Router) können auch mehrere Adressen zugeordnet werden. Der Begriff Host-Adresse bezeichnet die IP-Adresse des Rechners eines IP-Prozesses, unabhängig von der tatsächlichen physikalischen Struktur des Geräts oder der Schnittstellen.

7.1.2 IP-Adress-Struktur

IP-Adressen haben eine Länge von vier Oktetten, 32 Bits (4 Bytes), und werden in dezimaler oder hexadezimaler Schreibweise mit Punkt “.” getrennt notiert. Zum Beispiel:
198.10.6.27 oder
C6.0A.06.1B oder
0xC6.0x0A.0x06.0x1B

Die Adressen werden getrennt in einen Netzwerk-Abschnitt, der das zugehörige Netz adressiert, und eine lokale Adresse, dem sogenannten “Restfeld” (auch Host-Abschnitt), der das jeweilige Gerät innerhalb des Netzwerks adressiert. Alle Geräte innerhalb eines einzelnen Netzwerks haben denselben Netzwerk-Abschnitt gemeinsam. Jedes Gerät (Host) hat dabei sein eigenes Restfeld.

Es gibt drei Klassen von Internet-Adressen, je nachdem wieviele Bytes der IP-Adresse für Netzwerk-Abschnitt und Restfeld verwendet werden.

Klasse (Class) A, große Netzwerke: Netzwerknummern 1 - 127

Bei Adressen der Klasse A ist das höchste Bit gleich Null, die nächsten sieben Bits entsprechen dem Netzwerk und die verbleibenden 24 Bits der lokalen Adresse.

Netzwerk-Abschnitt beansprucht 1 Byte (max. 126 unterschiedliche Netzwerke)

Restfeld beansprucht 3 Bytes (max. $2^8 \cdot 2^8 \cdot 2^8 = 16.777.216$ verschiedene Geräte)

Damit können max. 127 unterschiedliche Netzwerke, jedes mit max. 16.777.216 verschiedenen Geräten, adressiert werden.

Klasse (Class) B, mittlere Netzwerke: Netzwerknummern 128 - 191

Bei Adressen der Klasse B haben die beiden höchsten Bits die Werte 1 und 0, die nächsten 14 Bits entsprechen dem Netzwerk und die verbleibenden 16 Bits der lokalen Adresse.

Netzwerk-Abschnitt beansprucht 2 Byte (max. 16.384 unterschiedliche Netzwerke)

Restfeld beansprucht 2 Bytes (max. $2 \text{ hoch } 16 = 65.536$ verschiedene Geräte)

Damit können max. 16.384 unterschiedliche Netzwerke, jedes mit max. 65.526 verschiedenen Geräten, adressiert werden.

Klasse (Class) C, kleine Netzwerke: Netzwerknummern 192 - 223

Bei Adressen der Klasse C haben die drei höchsten Bits die Werte 1, 1 und 0, die folgenden 21 Bits entsprechen dem Netzwerk und die letzten 8 Bits der lokalen Adresse.

Netzwerk-Abschnitt beansprucht 3 Bytes (max. 2.097.152 unterschiedliche Netzwerke)

Restfeld beansprucht 1 Byte (max. 256 verschiedene Geräte)

Damit können max. 2.097.152 unterschiedliche Netzwerke, jedes mit max. 256 verschiedenen Geräten, adressiert werden.

Beispiel:

	Net z	Host
Klasse A:	122 .	087 . 156 . 045
Klasse B:	162 .	143 . 085 . 132
Klasse C:	195 .	076 . 212 . 024

Bitte beachten Sie bei der Adressvergabe, dass für einen einzelnen physikalischen Rechner mehrere IP-Adressen verwendbar sein müssen. Eine Workstation kann mit einer IP-Adresse auskommen. Ein Router benötigt für jede seiner Schnittstellen eine IP-Adresse, mindestens jedoch zwei – eine für den Anschluss zum lokalen Netz (LAN IP-Adresse), eine für den Anschluss zur WAN-Seite.

7.1.3 Netzmasken (Subnet Masks)

In einem Wide Area Network können verschiedene, physikalisch getrennte Netze (LANs) dem gleichen Netzwerk (WAN) mit der gleichen Netzwerknummer angehören. Anhand dieser Netzwerknummer allein kann kein Router entscheiden, ob er bei einer IP-Kommunikation eine Verbindung zu einem physikalisch anderen Netz innerhalb des WANs aufbauen soll. Das Netzwerk (WAN) muss daher in kleinere Abschnitte (LANs) unterteilt werden, die einen eigenen Adressblock erhalten. Jeder Adressblock der einzelnen physikalischen Netze wird als Subnet bezeichnet. Durch diese Unterteilung eines Netzwerks in Subnets wird die Hierarchie aus Netzwerk und Rechner zu einer Hierarchie erweitert aus Netzwerk, Subnet und Rechner.

Diese erweiterte Hierarchie erleichtert zum einen das Auffinden eines Rechners im Gesamtnetz (WAN). Man kann sich dies vorstellen analog zur Nomenklatur im Telefonnetz, wo zum Beispiel die Ortsvorwahl aussagt in welchem Bereich sich ein Anschluss befindet. Diese Hierarchie gewährt auch eine gewisse Zugriffssicherheit. So kann in einem Firmennetz zum Beispiel der Rechner eines Subnets nicht ohne weiteres auf Ressourcen eines anderen Subnets zugreifen – etwa ein Mitarbeiter aus der Fertigungsabteilung auf Datenbestände aus der Personalabteilung – wenn die Netz-Masken nach Firmenabteilungen entsprechend gewählt sind.

Die Netz-Maske (Subnet Mask) gibt den Standort des Subnet-Felds in einer IP-Adresse an. Die Netz-Maske ist eine binäre 32-Bit-Zahl wie eine IP-Adresse. Sie hat eine "1" an allen Stellen des Netzwerk-Abschnitts der IP-Adresse (je nach Netzwerk-Klasse innerhalb des ersten bis dritten Oktetts). Das darauf folgende Oktett gibt die Position des Subnet-Feldes an. Die im Subnet-Feld an den Netzwerk-Abschnitt aufschließenden Einsen geben die Subnet-Bits an. Alle übrigen Stellen mit "0" verbleiben für den Host-Abschnitt.

■ Beispiele

Beispiel 1:

Die Netzmaske dient der Interpretation der IP-Adresse. So kann eine Adresse 135.96.7.230 mit der Maske 255.255.255.0 so interpretiert werden: Das Netzwerk hat die Adresse 135.96.0.0, das Subnet hat die Nummer 7, der Rechner Nummer 230. Eine IP-Adresse mit 135.96.4.190 gehört dem gleichen Netzwerk aber einem anderen Subnet (4) an.

Binäre Darstellung:

135.96.7.230	=	10000111	11000000		00000111		11100110
135.96.4.190	=	10100000	10010101		00000100		10111110
255.255.255.0	=	11111111	11111111		11111111		00000000
		Netzwerk			Subnet		
255.255.248.0	=	11111111	11111111		11111	000	00000000

Hätte die Netz-Maske in obigem Beispiel nicht den Standardwert 255.255.255.0, sondern 255.255.248.0, befänden sich die IP-Adressen im gleichen Subnet – und Routing würde nicht stattfinden.

Beispiel 2:

Zwei IP-Adressen mit 160.149.115.8 und 160.149.117.201 und der Netz-Maske 255.255.252.0 befinden sich im gleichen Netzwerk 160.149, gehören aber unterschiedlichen Subnets an.

Binäre Darstellung:

160.149.115.8	=	10100000	10010101		011100		11	00001000
160.149.117.201	=	10100000	10010101		011101		01	11001001
255.255.252.0	=	11111111	11111111		111111		00	00000000
		Netzwerk					Subnet	

Die Wahl einer geeigneten Netzmaske hängt von der Netzwerk-Klasse, der Beschaffenheit der möglichen Subnets, ihrer Anzahl und ihrem Wachstum ab. Ziehen Sie zur Planung einschlägige Tabellen oder einen Subnet-Taschenrechner zu Rate.

Subnet-Tabelle Klasse C:

Subnet-Bits	Host-Bits	Netz-Maske	Subnets	Rechner
2	6	255.255.255.192	2	62
3	5	255.255.255.224	6	30
4	4	255.255.255.240	14	14
5	3	255.255.255.248	30	6
6	2	255.255.255.252	62	2

(Berechnung: 2 hoch n minus 2 = Anzahl der Subnets/Rechner
n: Anzahl der Subnet/Host-Bits)

Mit einer Netz-Maske 255.255.255.240 wird ein Netz der Klasse C in Subnets geteilt. Mit dieser Netz-Maske sind insgesamt 14 Subnets mit jeweils max. 14 Rechnern möglich.

255.255.255.240	11111111	11111111	11111111		1111		0000	
199. 9. 99.130	11000111	00001001	01100011		1000		0010	Subnet-Nummer 8
199. 9. 99.146	11000111	00001001	01100011		1001		0010	Subnet-Nummer 9
	Netzwerk				Subnet		Host	

■ Standard-Masken

Netzmaske für Klasse A: 255. 0. 0. 0

Netzmaske für Klasse B: 255. 255. 0. 0

Netzmaske für Klasse C: 255. 255. 255. 0

■ Reservierte Adressen

Einige IP-Adressen dürfen Geräten eines Netzwerks nicht zugeordnet werden. Dazu gehören die Netzwerk- oder Subnet-Adresse und die Rundsendungsadresse für Netzwerke bzw. Subnets. Netzwerk-Adressen bestehen aus der Netzwerknummer und dem Host-Feld, das mit binären Nullen gefüllt ist (z.B. 200.1.2.0, 162.66.0.0., 10.0.0.0) – auch Loop Back, es findet keine Übertragung ins Netzwerk statt. Die Rundsendungsadresse eines Netzwerks besteht aus der Netzwerknummer und dem Host-Feld mit binären Einsen (z.B. 200.1.2.255, 162.66.255.255., 10.255.255.255) – daher auch “All One Broadcast”, alle Stationen eines Netzwerks werden adressiert.

Beispiel:

198.10.2.255	adressiert alle Stationen im Netz 198.10.2.
255.255.255.255	adressiert alle Stationen in allen angeschlossenen Netzen
0.0.0.0	All Zero Broadcast: Ungültige Adresse.

Bitte beachten Sie, dass diese Adresse oft für Standard-Einstellungen benutzt wird.

7.1.4 Zum Umgang mit IP-Adressen

- ☐ Jede IP-Adresse im unternehmensweiten Netz sollte nur einmalig vorhanden sein. Beachten Sie dies bei Internet-Anschluss und Anschluss neuer Netze.
- ☐ Benutzen Sie ein nachvollziehbar logisches Schema bei der Adress-Vergabe, z.B. Verwaltungseinheiten, Gebäude, Abteilungen etc.
- ☐ Für den Anschluss ans Internet benötigen Sie eine offizielle einmalige Internet-Adresse.
- ☐ Vergeben Sie, wenn möglich, keine IP-Adresse, deren Netzwerk- oder Host-Abschnitt mit “0” endet. Dies könnte zu Fehlinterpretationen und undefinierbaren Fehlern im Netz führen.
- ☐ Netzmasken werden vom Internet-Protokoll nur ausgewertet, wenn die Netzwerknummern der Kommunikationspartner gleich sind.
- ☐ Wie die Adress-Klassen haben auch die Netz-Masken unterschiedlich lange Netzwerk-Abschnitte.

7.2 Security



Im Parameterfeld “IPSec-Einstellungen” der Profil-Einstellungen sind die Konfigurationsparameter zu IPSec für den Einsatz in Remote Access-Umgebungen gesammelt. Im folgenden wird auf einige Konfigurationsmöglichkeiten Bezug genommen.

7.2.1 IPSec – Übersicht

IPSec kann nur für IP-Datenverkehr eingesetzt werden. Die IPSec-Spezifikation umfasst nicht nur das (Layer 3-) Tunneling, sondern auch alle notwendigen Sicherheitsmechanismen, wie starke Authentisierung, Schlüsselaustausch und Verschlüsselung.

Mit den IPSec RFCs (2401 - 2409) lässt sich ein VPN mit vorgegebener Security für IP realisieren. Tunneling und Security sind für IPSec vollständig beschrieben, so dass ein komplettes Rahmenwerk für das VPN zur Verfügung steht. Prinzipiell ist es möglich, herstellerunabhängige verschiedene Komponenten zu nutzen. In Site to Site VPNs etwa könnten die VPN Gateways von verschiedenen Herstellern stammen, in End to Site VPNs könnten die Clients von einem anderen Hersteller als die Gateways sein.

Der Verbindungsaufbau zum IPSec-Verkehr erfolgt auf Basis des Internet Key Exchange-Protokolls (IKE).

■ IPSec – allgemeine Funktionsbeschreibung

In jedem IP-Host (Client oder Gateway) der IPSec unterstützt, gibt es ein IPSec-Modul, bzw. eine IPSec-Maschine. Dieses Modul untersucht jedes IP-Paket nach bestimmten Eigenschaften, um die jeweils entsprechende Security-Behandlung darauf anzuwenden.

Die Prüfung der vom IP Stack ausgehenden IP-Pakete erfolgt bezüglich einer Secure Policy Database (SPD). Dabei werden alle konfigurierten SPDs abgearbeitet. (Bei Einsatz des IPSec Clients werden die SPDs nur zentralseitig am Gateway gehalten.)

Die SPD besteht aus mehreren Einträgen (SPD Entries), die wiederum einen Filterteil beinhalten. Der Filterteil (siehe → Erweiterte Firewall-Einstellungen) oder Selektor eines SPD-Eintrags besteht hauptsächlich aus IP-Adressen, UDP und TCP Ports sowie anderer IP Header-spezifischer Einträge. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des SPD-Eintrags übereinstimmen, wird aus den SPD-Einträgen weiter ermittelt, wie mit diesem IP-Paket zu verfahren ist. Das Paket kann einfach durchgelassen werden (permit), es kann abgelehnt bzw. weggeworfen werden (deny) oder bestimmte Security-Richtlinien des IPSec-Prozesses kommen an ihm zur Anwendung. Diese Security-Richtlinien stehen auch im SPD-Eintrag beschrieben.

Wird auf diese Weise festgestellt, dass ein IP-Paket mit einem SPD-Eintrag verknüpft ist, der einen IPSec-Prozess einleitet, so wird überprüft, ob bereits eine Sicherheits-

Verknüpfung (Security Association, SA) für diesen SPD-Eintrag existiert. Existiert noch keine SA, wird vor dem Aushandeln einer SA zunächst eine Authentisierung und ein Schlüsselaustausch (siehe unten → IPSec-Verhandlung Phase 1) vorgenommen.

Nach der SA-Verhandlung erfolgen in einem weiteren Schritt (siehe unten → IPSec-Verhandlung Phase 2) die Verhandlungen für eine Verschlüsselung (ESP) und/oder Authentisierung (AH) der Datenpakete.

Die SA beschreibt, welches Sicherheitsprotokoll verwendet werden soll. ESP (Encapsulating Security Payload) unterstützt die Verschlüsselung und die Authentisierung von IP-Paketen, AH (Authentication Header) unterstützt nur die Authentisierung von IP-Paketen. Die SA beschreibt auch, in welcher Betriebsart das Sicherheitsprotokoll benutzt werden soll (Tunnel- oder Transportmodus). Im Tunnelmodus wird ein IP Header hinzugefügt, im Transportmodus wird der Original-Header verwendet. Weiter beschreibt die SA, welcher Algorithmus zur Authentisierung verwendet werden soll, welche Verschlüsselungsmethode (bei ESP) und welcher Schlüssel zur Anwendungen kommen sollen. Die Gegenstelle muss selbstverständlich nach der gleichen SA arbeiten.

Ist die SA ausgehandelt, wird jedes Datenpaket gemäß Betriebsmodus (Tunnel oder Transport) und Protokoll (ESP oder AH) bearbeitet. Der IPSec Client nutzt immer das ESP-Protokoll im Tunnelmodus.

7.2.2 Firewall-Einstellungen / Firewall Settings

Die Firewall-Einstellungen bestehen hauptsächlich aus IP-Adressen, UDP und TCP Ports sowie anderer IP Header-spezifischer Einträge. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des Regel-Eintrags übereinstimmen, wird aus den Regel-Einträgen weiter ermittelt, wie mit diesem IP-Paket zu verfahren ist.

Im folgenden die Einträge zur Konfiguration im IPSec Client:

☐ Ausführung / Command

gestatten (permit), sperren (deny), inaktiv (disabled)

☐ IP-Protokoll / IP Protocol

Dies ist das Transportprotokoll (ICMP, TCP oder UDP). Eines der angebotenen Protokolle kann ausgewählt werden oder ein beliebiges (alle / any) wird genutzt.

☐ IP-Adresse (Quelle) / Source IP Address

Dies kann eine einfache IP-Adresse oder ein Adressbereich sein. Letzteres ist nötig, wenn mehrere Ausgangssysteme mit einer gemeinsamen SA unterstützt werden sollen (z.B. hinter einer Firewall).

☐ IP-Adresse (Ziel) / Destination IP Address

Dies kann eine einfache IP-Adresse oder ein Adressbereich sein. Letzteres ist nötig, wenn mehrere Zielsysteme mit einer gemeinsamen SA unterstützt werden sollen (z.B. hinter einer Firewall).

☐ Port (Quelle) / Source Port

Dies können einzelne TCP- oder UDP-Portnummern oder ein Bereich von Portnummern sein. Die Portnummern mit zugeordnetem Service bestimmen Sie über den Auswahlbutton [...].

☐ Port (Ziel) / Destination Port

Dies können einzelne TCP- oder UDP-Portnummern oder ein Bereich von Portnummern sein. Die Portnummern mit zugeordnetem Service bestimmen Sie über den Auswahlbutton [...].

7.2.3 SA-Verhandlung und Richtlinien / Policies

Damit der IPSec-(Filter-)Prozess in Gang kommen kann, müssen vorher verschiedene SAs verhandelt worden sein. Es wird eine SA für Phase 1 (IKE-Richtlinie) sowie mindestens zwei (je für ein- und ausgehende Verbindung) für Phase 2 (IPSec-Richtlinie) ausgehandelt. [Für jedes Zielnetz (siehe → Profil-Einstellungen, VPN Networks) werden ebenfalls zwei SAs ausgehandelt.]

■ Phase 1 (Parameter der IKE-Richtlinie / IKE Policy):

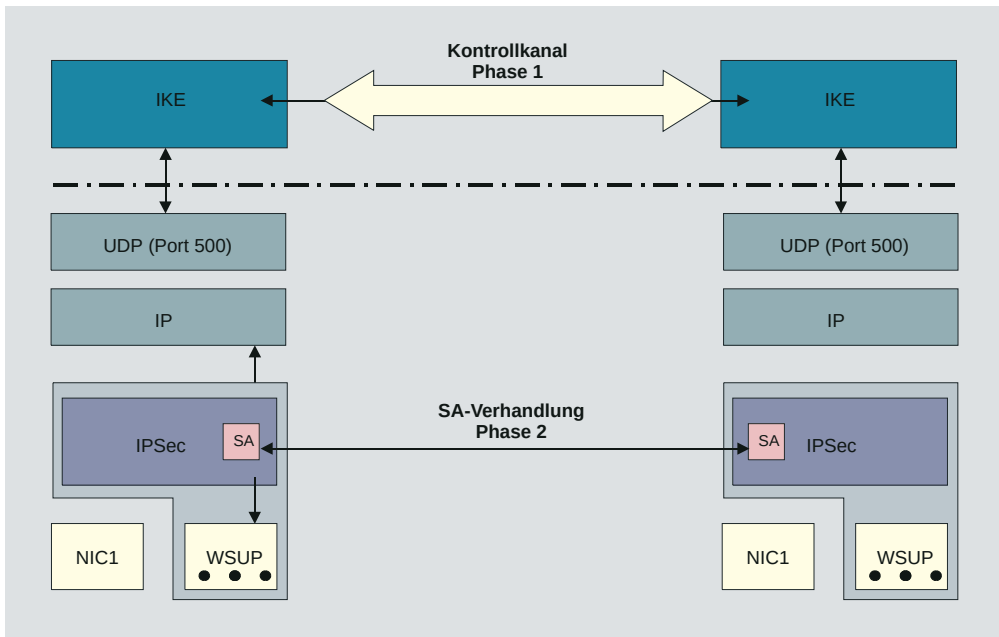
Der Kontrollkanal wird im Tunnelmodus von IPSec über das IKE-Protokoll zur IP-Adresse des Gateways aufgebaut, im Transportmodus direkt zur IP-Adresse der Gegenstelle.

Parameter zur Festlegung von Verschlüsselungs- und Authentisierungsart über das IKE-Protokoll definieren Sie in den IKE-Richtlinien. Dabei kann die Authentisierung über einen Pre-shared Key oder eine RSA Signatur erfolgen. (Entsprechende Richtlinien sind im Richtlinien-Editor vorkonfiguriert.)

■ Phase 2 (Parameter der IPSec-Richtlinie / IPSec Policy):

Die SA-Verhandlung wird über den Kontrollkanal abgewickelt. Von der IPSec-Maschine wird die SA an das IKE-Protokoll übergeben, das sie über den Kontrollkanal zur IPSec-Maschine der Gegenstelle überträgt.

Kontrollkanal und SA-Verhandlung



Bildbeschreibung:

Damit der IPsec-Prozess in Gang kommen kann, muss vorher die SA verhandelt worden sein. Diese SA-Verhandlung findet pro SPD – die für verschiedene Ports, Adressen und Protokolle angelegt sein können – einmal statt. Für diese SA-Verhandlung wird ein Kontrollkanal benötigt.

Im Client muss nun zunächst eine Layer 2-(PPP)-Verbindung zum Provider hergestellt werden. Dabei bekommt er (bei jeder Einwahl) eine neue IP-Adresse. Das IPsec-Modul im Client bekommt ein IP-Paket mit der Zieladresse der Firmenzentrale. Ein SPD-Eintrag für dieses IP-Paket wird gefunden aber es existiert noch keine SA. Das IPsec-Modul stellt die Anforderung an das IKE-Modul, eine SA auszuhandeln. Dabei werden auch die angeforderten Sicherheits-Richtlinien, wie sie im SPD-Eintrag vorhanden sind, an das IKE-Modul übergeben. Eine IPsec-SA auszuhandeln wird als Phase-2-Verhandlung bezeichnet. Bevor jedoch eine IPsec-SA mit der Gegenstelle (Gateway) ausgehandelt werden kann, muss ein Kontrollkanal vom Client zum Gateway existieren. Dieser Kontrollkanal wird über die Phase-1-Verhandlung hergestellt, deren Ergebnis eine IKE-SA ist. Die Phase-1-Verhandlung übernimmt somit die komplette Authentisierung vom Client gegenüber dem VPN Gateway und erzeugt einen verschlüsselten Kontrollkanal. Über diesen Kontrollkanal kann dann rasch die Phase 2 (IPsec SA) durchgeführt werden. Die Phase-1-Verhandlung ist ein Handshake, über den auch der Austausch von Zertifikaten möglich ist und die den Schlüsselaustausch für den Kontrollkanal beinhaltet.

IKE-Modi

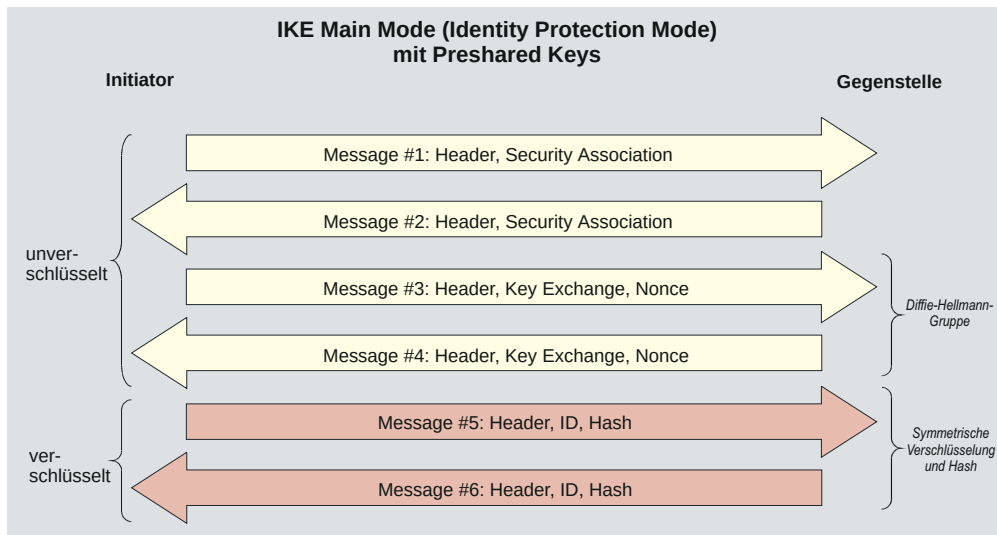
Im wesentlichen können zwei Arten der IKE-Richtlinien konfiguriert werden. Sie unterscheiden sich durch die Art der Authentisierung, entweder über Pre-shared Key oder über RSA-Signatur. Beide Arten des Internet Key Exchanges können in zwei unterschiedlichen Modi ausgeführt werden, dem Main Mode, auch Identity Protection Mode, oder dem Aggressive Mode. Die Modi unterscheiden sich durch die Anzahl der Messages und durch die Verschlüsselung.

Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden – daher auch Identity Protection Mode.

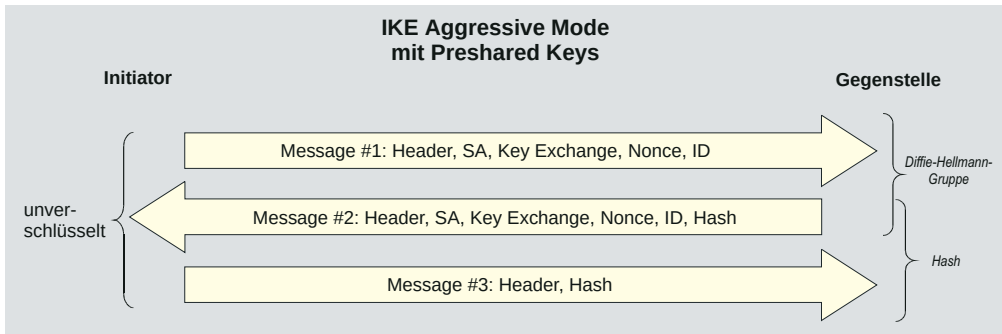
Im Aggressive Mode gehen nur drei Meldungen über den Kontrollkanal, wobei nichts verschlüsselt wird.



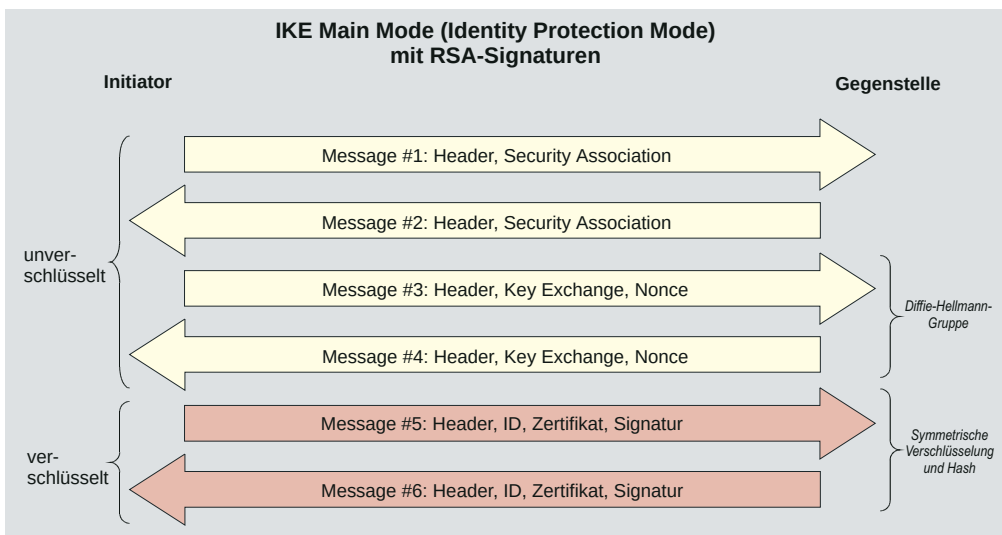
Den IKE-Modus (Austausch-Modus / Exchange Mode), Main Mode oder Aggressive Mode, bestimmen Sie in den Profil-Einstellungen im Parameterfeld "IPSec-Einstellungen".



Wird die Pre-shared Key-Methode im Main Mode genutzt (Bild oben), so muss der Client am VPN/GW durch seine IP-Adresse eindeutig identifizierbar sein, da der Pre-shared Key mit in die symmetrische Schlüsselberechnung einbezogen und verschlüsselt wird, bevor sonstige Informationen übertragen werden, die den Client identifizieren könnten. Ein Client, der sich beim Provider einwählt, ist jedoch nicht durch die IP-Adresse zu erkennen, da er bei jeder Provider-Anwahl eine neue zugewiesen bekommt. Letztlich kann im Main Mode an alle Clients nur derselbe Pre-shared Key vergeben werden, was allerdings die Authentisierung abschwächt.



Eine Möglichkeit, einen allgemeinen Pre-shared Key zu vermeiden, wäre, den Aggressive Mode zu nutzen (Bild oben), doch wird dabei die ID des Clients nicht verschlüsselt.



Werden RSA-Signaturen eingesetzt (Bild oben und unten), so bedeutet dies, dass Zertifikate zum Einsatz kommen, womit die Vorkonfiguration jedweder "Secrets" überflüssig wird.



7.2.4 IPSec Tunneling

Der IPSec Client kann gegenüber IPSec-Gateways unterschiedlicher anderer Hersteller zum Einsatz kommen.

Die Kompatibilität mit den IPSec-Modi der anderen Hersteller beruht auf der Konformität mit folgenden RFCs und Drafts zu IPSec:

RFC 2104 - Keyed-Hashing for Message Authentication
RFC 2401 - Security Architecture for the Internet Protocol
RFC 2403 - The Use of HMAC-MD5-96 within ESP and AH
RFC 2404 - The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2406 - IP Encapsulating Security Payload (ESP)
RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409 - The Internet Key Exchange (IKE)
DRAFT - draft-beaulieu-ike-xauth-05 (XAUTH)
DRAFT - draft-dukes-ike-mode-cfg-02 (IKECFG)
DRAFT - draft-ietf-ipsec-dpd-01 (DPD)
DRAFT - draft-ietf-ipsec-nat-t-ike-01 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-02 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-03 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-05 (NAT-T)
DRAFT - draft-ietf-ipsec-udp-encaps-06 (UDP-ENCAP)

■ Implementierte Algorithmen für Phase 1 und 2:

Unterstützte Authentisierung für Phase 1 (IKE-Richtlinie)

- RSA-Signatur
- PSK (Pre-shared Key)

Unterstützte symmetrische Verschlüsselungsalgorithmen (Phase 1 + 2)

- DES
- 3DES
- AES-128, AES-192, AES-256

Unterstützte asymmetrische Verschlüsselungsalgorithmen (Phase 1 + 2)

- DH 1,2,5 (Diffie-Hellmann)
- RSA

Unterstützte Hash-Algorithmen

- MD5
- SHA-1

Zusätzliche Unterstützung für Phase 2

- PFS (Perfect Forward Secrecy)
- IPCOMP (LZS)
- Seamless re-keying

In den Profil-Einstellungen des IPSec Clients werden automatisch einige Standards gesetzt:

- IKE Phase 1 Richtlinie - Automatischer Modus
- IKE Phase 2 Richtlinie - Automatischer Modus
- IKE Phase 1 Modus RSA - Main Mode
- IKE Phase 1 Modus PSK - Aggressive Mode



Diese automatisch gesetzten Richtlinien und Verhandlungsmodi sind in den Profil-Einstellungen konfigurierbar gehalten, sodass sie anderslautenden Verbindungsanforderungen entsprechend modifiziert werden können.

Standard IKE-Vorschläge:



1. Wenn für die IKE-Richtlinie der automatische Modus in den IPSec-Einstellungen gewählt wurde und im Parameterfeld "Identität" die Verwendung eines Pre-shared Keys nicht aktiviert wurde (ohne Haken!), so werden an die Gegenstelle standardmäßig folgende Vorschläge für die IKE-Richtlinie versendet, wobei die Authentisierung immer mit Zertifikat erfolgt:

Notation:

EA = Encryption Algorithm (Verschlüsselung)
 HASH = Hash Algorithm (Hash)
 AUTH = Authentication Method (Authentisierung)
 GROUP = Diffie-Hellmann Group Number (DH-Gruppe)
 LT = Life Type (Dauer)
 LS = Life Seconds (Dauer)
 KL = Key Length (Schlüssellänge)

EA	HASH	AUTH	GROUP	LT	LS	KL
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	256
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	256
AES_CBC	SHA	RSA	DH5	SECONDS	28800	256
AES_CBC	MD5	RSA	DH5	SECONDS	28800	256
AES_CBC	SHA	XAUTH_RSA	DH2	SECONDS	28800	256
AES_CBC	MD5	XAUTH_RSA	DH2	SECONDS	28800	256
AES_CBC	SHA	RSA	DH2	SECONDS	28800	256
AES_CBC	MD5	RSA	DH2	SECONDS	28800	256
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	192
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	192
AES_CBC	SHA	RSA	DH5	SECONDS	28800	192
AES_CBC	MD5	RSA	DH5	SECONDS	28800	192
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	128
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	128
AES_CBC	SHA	RSA	DH5	SECONDS	28800	128
AES_CBC	MD5	RSA	DH5	SECONDS	28800	128
AES_CBC	SHA	XAUTH_RSA	DH2	SECONDS	28800	128
AES_CBC	MD5	XAUTH_RSA	DH2	SECONDS	28800	128
AES_CBC	SHA	RSA	DH2	SECONDS	28800	128
AES_CBC	MD5	RSA	DH2	SECONDS	28800	128
DES3	SHA	XAUTH_RSA	DH5	SECONDS	28800	0
DES3	MD5	XAUTH_RSA	DH5	SECONDS	28800	0
DES3	SHA	RSA	DH5	SECONDS	28800	0
DES3	MD5	RSA	DH5	SECONDS	28800	0
DES3	SHA	XAUTH_RSA	DH2	SECONDS	28800	0
DES3	MD5	XAUTH_RSA	DH2	SECONDS	28800	0
DES3	SHA	RSA	DH2	SECONDS	28800	0
DES3	MD5	RSA	DH2	SECONDS	28800	0



Wird ein spezifischer IKE-Vorschlag in der IPSec-Konfiguration der Profil-Einstellungen eingestellt, so wird immer auch automatisch der gleiche Vorschlag zusätzlich mit Extended Authentication generiert und versendet.

2. Wird in das Feld für “Pre-shared Key” ein String eingetragen, so werden an die Gegenstelle standardmäßig folgende Vorschläge für die IKE-Richtlinie versendet, wobei die Authentisierung immer ohne Zertifikat erfolgt:

EA	HASH	AUTH	GROUP	LT	LS	KL
AES_CBC	SHA	XAUTH_PSK	DH5	SECONDS	28800	256
AES_CBC	MD5	XAUTH_PSK	DH5	SECONDS	28800	256
AES_CBC	SHA	PSK	DH5	SECONDS	28800	256
AES_CBC	MD5	PSK	DH5	SECONDS	28800	256
AES_CBC	SHA	XAUTH_PSK	DH2	SECONDS	28800	256
AES_CBC	MD5	XAUTH_PSK	DH2	SECONDS	28800	256
AES_CBC	SHA	PSK	DH2	SECONDS	28800	256
AES_CBC	MD5	PSK	DH2	SECONDS	28800	256
AES_CBC	SHA	XAUTH_PSK	DH5	SECONDS	28800	192
AES_CBC	MD5	XAUTH_PSK	DH5	SECONDS	28800	192
AES_CBC	SHA	PSK	DH5	SECONDS	28800	192
AES_CBC	MD5	PSK	DH5	SECONDS	28800	192
AES_CBC	SHA	XAUTH_PSK	DH5	SECONDS	28800	128
AES_CBC	MD5	XAUTH_PSK	DH5	SECONDS	28800	128
AES_CBC	SHA	PSK	DH5	SECONDS	28800	128
AES_CBC	MD5	PSK	DH5	SECONDS	28800	128
AES_CBC	SHA	XAUTH_PSK	DH2	SECONDS	28800	128
AES_CBC	MD5	XAUTH_PSK	DH2	SECONDS	28800	128
AES_CBC	SHA	PSK	DH2	SECONDS	28800	128
AES_CBC	MD5	PSK	DH2	SECONDS	28800	128
DES3	SHA	XAUTH_PSK	DH5	SECONDS	28800	0
DES3	MD5	XAUTH_PSK	DH5	SECONDS	28800	0
DES3	SHA	PSK	DH5	SECONDS	28800	0
DES3	MD5	PSK	DH5	SECONDS	28800	0
DES3	SHA	XAUTH_PSK	DH2	SECONDS	28800	0
DES3	MD5	XAUTH_PSK	DH2	SECONDS	28800	0
DES3	SHA	PSK	DH2	SECONDS	28800	0
DES3	MD5	PSK	DH2	SECONDS	28800	0

Als Vorschläge für die IPSec-Richtlinie (Phase 2) wird standardmäßig versendet:

Notation:

PROTO	-	Protocol (Protokoll)
TRANS	-	Transform (Transformation (ESP))
LT	-	Life Type (Dauer)
LS	-	Life Seconds (Dauer)
KL	-	Key Length (Schlüssellänge)
COMP	-	IP Compression (Transformation (Comp))

PROTO	TRANS	AUTH	LT	LS	KL	COMP	LZS
ESP	AES	MD5	SECONDS	28800	128	Yes	Yes
ESP	AES	SHA	SECONDS	28800	128	Yes	Yes
ESP	AES	MD5	SECONDS	28800	128	No	No
ESP	AES	SHA	SECONDS	28800	128	No	No
ESP	AES	MD5	SECONDS	28800	192	Yes	Yes
ESP	AES	SHA	SECONDS	28800	192	Yes	Yes
ESP	AES	MD5	SECONDS	28800	192	No	No
ESP	AES	SHA	SECONDS	28800	192	No	No
ESP	AES	MD5	SECONDS	28800	256	Yes	Yes
ESP	AES	SHA	SECONDS	28800	256	Yes	Yes
ESP	AES	MD5	SECONDS	28800	256	No	No
ESP	AES	SHA	SECONDS	28800	256	No	No
ESP	DES3	MD5	SECONDS	28800	0	Yes	Yes
ESP	DES3	MD5	SECONDS	28800	0	No	No

7.2.5 Zur weiteren Konfiguration

Pre-shared Key oder *RSA-Signatur*: Entsprechend den Vorgaben durch die Gegenstelle kann als "IKE-Richtlinie" die automatisch vorgenommene Einstellung "Automatischer Modus" auf "Pre-shared Key" oder "RSA Signatur" (Zertifikat) abgeändert werden. Erwartet die Gegenstelle "Pre-shared Key", so muss der Schlüssel in das Feld eingetragen werden. (Der Pre-shared Key muss in diesem Fall für alle Clients identisch sein.)

IP-Adressen und *DNS Server* können über das Protokoll IKE-Config Mode (Draft 2) zugewiesen werden. Für die NAS-Einwahl können alle üblichen WAN-Schnittstellen verwendet werden.

Die *Authentisierung* bei IPSec Tunneling kann über das XAUTH Protokoll (Draft 6) erfolgen. Dazu müssen außerdem noch folgende Parameter im Konfigurationsfeld "Identität" gesetzt werden:

Benutzername	=	Kennwort des IPSec-Benutzers
Passwort	=	Passwort des IPSec-Benutzers
Zugangsdaten aus ... verwenden	=	optional

Bei IPSec Tunneling wird im Hintergrund automatisch DPD (Dead Peer Detection) und NAT-T (NAT Traversal) ausgeführt, falls dies von der Gegenstelle unterstützt wird. Mit DPD prüft der IPSec Client in bestimmten Abständen, ob die Gegenstelle noch aktiv ist. Bei inaktiver Gegenstelle erfolgt ein automatischer Verbindungsabbau. Unterstützt die Gegenstelle DPD nicht, so kann DPD im Parameterfeld "IPSec-Einstellungen" deaktiviert werden. Der Einsatz von NAT Traversal erfolgt beim IPSec Client automatisch und ist immer nötig, wenn auf dem Weg zum Zielsystem ein Gerät mit Network Address Translation zum Einsatz kommt.

■ Basiskonfigurationen in Abhängigkeit vom IPSec Gateway

Im folgenden sind Konfigurationsmöglichkeiten aufgeführt, die zu beachten sind, je nachdem ob das IPSec Gateway Extended Authentication (XAUTH) und IKE-Config Mode unterstützt oder nicht.

Gateway unterstützt nicht XAUTH

Der IPSec Client als Initiator der IPSec-Verbindung schlägt standardmäßig immer die Extended Authentication vor. Diese Eigenschaft kann nicht konfiguriert werden. Unterstützt das Gateway die Extended Authentication nicht, so wird sie auch nicht durchgeführt.

Gateway unterstützt IKE-Config Mode

Sofern das Gateway den IKE-Config Mode unterstützt, kann im Parameterfeld "IP-Adressen-Zuweisung" die Funktion "IKE Config Mode verwenden" aktiviert werden.

Gateway unterstützt IKE-Config Mode nicht

Unterstützt das Gateway den IKE-Config Mode nicht, so sind zwei Konfigurationen möglich.

1. Wird die Funktion "IP-Adresse manuell vergeben" (siehe → Profil-Einstellungen, IP-Adressen-Zuweisung) aktiviert, so muss die IP-Adresse eingetragen werden, die vom Gateway bzw. Administrator für diesen Client bzw. Benutzer vorgegeben wurde.
2. Wird "Lokale IP-Adresse verwenden" (siehe → Profil-Einstellungen, IP-Adressen-Zuweisung) aktiviert, so wird die IP-Adresse gleich der öffentlichen IP-Adresse gesetzt, die der Client pro Internet Session vom Provider erhält oder, unter der Verbindungsart "LAN", die Adresse, die der LAN-Adapter besitzt.

Wird die lokale IP-Adresse verwendet und der "Typ" im Parameterfeld "Identität" steht auf "IP-Adresse", dann darf im Feld für die "ID" keine IP-Adresse eingetragen sein. Nur dann ist gewährleistet, dass die jeweils aktuelle öffentliche IP-Adresse automatisch zur Identifikation für Phase 1 an das Gateway übertragen wird.

7.2.6 IPSec Ports für Verbindungsaufbau und Datenverkehr

Bitte beachten Sie, dass der IPSec Client exklusiven Zugriff auf den UDP Port 500 benötigt. Sofern NAT Traversal eingesetzt wird, wird auch Zugriff auf Port 4500 benötigt. Ohne NAT Traversal wird das IP-Protokoll ESP (Protokoll-ID 50) benutzt.

Standardmäßig wird der Port 500, der für den Verbindungsaufbau genutzt wird, unter Windows-Systemen von den IPSec-Richtlinien genutzt. Um dies zu ändern gehen Sie wie folgt vor:

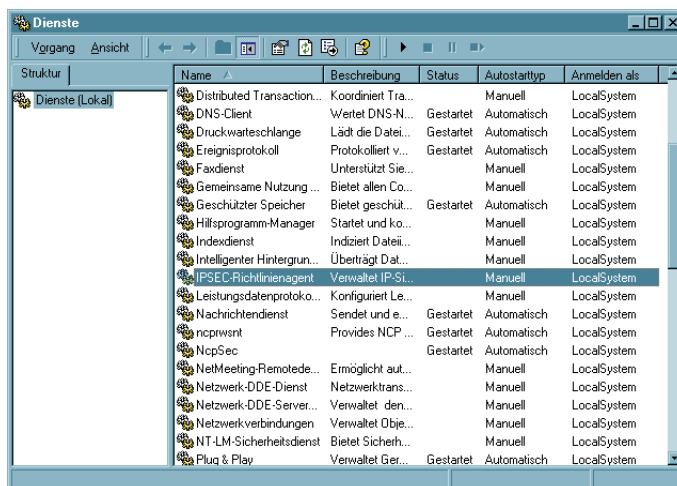
1. Um sich zu vergewissern, welche Ports aktuell von Ihrem System genutzt werden, können Sie unter der MS-DOS-Eingabeaufforderung mit dem Kommando `netstat -n -a` den aktuellen Netzstatus anzeigen lassen. In der Abbildung rechts erkennen Sie, dass der UDP Port 500 genutzt wird.

F:\>netstat -n -a

Aktive Verbindungen

Proto	Lokale Adresse	Remoteadresse	Status
TCP	0.0.0.0:135	0.0.0.0:0	ABHÖREN
TCP	0.0.0.0:445	0.0.0.0:0	ABHÖREN
TCP	0.0.0.0:1025	0.0.0.0:0	ABHÖREN
TCP	0.0.0.0:1032	0.0.0.0:0	ABHÖREN
TCP	0.0.0.0:5000	0.0.0.0:0	ABHÖREN
TCP	172.16.113.140:139	0.0.0.0:0	ABHÖREN
TCP	172.16.113.140:1032	62.153.165.34:21	HERGESTELLT
UDP	0.0.0.0:135	*:*	
UDP	0.0.0.0:162	*:*	
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:1027	*:*	
UDP	0.0.0.0:1028	*:*	
UDP	127.0.0.1:123	*:*	
UDP	127.0.0.1:1900	*:*	
UDP	172.16.113.140:123	*:*	
UDP	172.16.113.140:137	*:*	
UDP	172.16.113.140:138	*:*	
UDP	172.16.113.140:1900	*:*	

2. Wird der Port genutzt, so muss im Windows-Startmenü das Fenster "System → Dienste-Verwaltung" geöffnet werden. Dort wird der "IPSEC-Richtlinienagent" markiert, der Dienst gestoppt und der "Autostarttyp" auf "Manuell" gestellt (Bild rechts).
3. Wurde die Änderung des Autostarttyps durchgeführt, so kann das Kommando



`netstat -n -a` erneut ausgeführt werden. Der UDP Port 500 darf dann unter den aktiven Verbindungen nicht mehr aufgeführt sein.

7.3 Zertifikats-Überprüfungen

Neben der Zertifikats-Überprüfung nach Inhalten erfolgt am IPSec Client eine weitere Zertifikatsprüfung in mehrfacher Hinsicht.

7.3.1. Auswahl der CA-Zertifikate

Der Administrator des Firmennetzes legt fest, welchen Ausstellern von Zertifikaten vertraut werden kann. Dies geschieht dadurch, dass er die CA-Zertifikate seiner Wahl in das Windows-Verzeichnis `\ncple\cacerts\` spielt. Das Einspielen kann bei einer Software-Distribution mit Disketten automatisiert stattfinden, wenn sich die Aussteller-Zertifikate bei der Installation der Software im Root-Verzeichnis der ersten Diskette befinden (siehe → CA-Zertifikate anzeigen).

Derzeit werden die Formate *.pem und *.crt für Aussteller-Zertifikate unterstützt. Sie können im Monitor unter dem Hauptmenüpunkt “Verbindung – Zertifikate – CA-Zertifikate anzeigen” eingesehen werden.

Wird am IPSec Client das Zertifikat einer Gegenstelle empfangen, so ermittelt der NCP Client den Aussteller und sucht anschließend das Aussteller-Zertifikat, zunächst auf Smart Card oder PKCS#12-Datei, anschließend im Verzeichnis `NCPL\CACERTS\`. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande. Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen.

7.3.2. Überprüfung der Zertifikats-Erweiterung

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zertifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben. Für den IPSec Client und das Gateway sind drei Erweiterungen von Bedeutung:

- ☐ extendedKeyUsage
- ☐ subjectKeyIdentifier
- ☐ authorityKeyIdentifier

■ **extendedKeyUsage**

Beindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung `extendedKeyUsage` so prüft der IPSec Client, ob der definierte erweiterte Verwendungszweck "SSL-Server-Authentisierung" enthalten ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung `extendedKeyUsage` vorhanden ist, den Verwendungszweck "SSL-Server-Authentisierung" beinhalten muss. Dies gilt auch bei einem Rückruf an den Client über VPN.

Ausnahme: Bei einem Rückruf des Servers an den Client nach einer Direkteinwahl ohne VPN aber mit PKI prüft der Server das Zertifikat des Clients auf die Erweiterung `extendedKeyUsage`. Ist diese vorhanden, muss der Verwendungszweck "SSL-Server-Authentisierung" beinhalten sein, sonst wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

■ **subjectKeyIdentifier / authorityKeyIdentifier**

Ein `keyIdentifier` ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der `authorityKeyIdentifier` (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem `subjectKeyIdentifier` (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann keine Übereinstimmung erkannt werden, wird die Verbindung abgelehnt.

Der `keyIdentifier` kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des `keyIdentifier`s eine größere Flexibilität zum Auffinden eines Zertifizierungspfades.

(Außerdem müssen die Zertifikate, die den `keyIdentifier` in der `authorityKeyIdentifier`-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.)

7.3.3. Überprüfung von Sperrlisten

Zu jedem Aussteller-Zertifikat kann dem IPSec Client die zugehörige CRL (Certificate Revocation List) zur Verfügung gestellt werden. Sie wird in das Windows-Verzeichnis `\ncple\crls\` gespielt. Ist eine CRL vorhanden, so überprüft der IPSec Client eingehende Zertifikate daraufhin, ob sie in der CRL geführt sind. Gleiches gilt für eine ARL (Authority Revocation List), die in das Windows-Verzeichnis `\ncple\arls\` gespielt werden muss.

7.4 Stateful Inspection-Technologie für die Firewall-Einstellungen

Die Firewall-Technologie der Stateful Inspection kann für alle Netzwerkadapter wie auch für RAS-Verbindungen eingesetzt werden. Sie wird am Client im Telefonbuch unter “Firewall-Einstellungen” aktiviert (siehe → Konfigurations-Parameter, Firewall-Einstellungen). Am Gateway ist sie dann aktiv, wenn im Server Manager unter “Routing Interfaces – Allgemein” die Funktion “LAN-Adapter schützen” eingeschaltet wird.

Grundsätzliche Aufgabe einer Firewall ist es, zu verhindern, dass sich Gefahren aus anderen bzw. externen Netzen (Internet) in das eigene Netzwerk ausbreiten. Deshalb wird eine Firewall auch am Übergang zwischen Firmennetz und z.B. Internet installiert. Sie prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis vorher festgelegter Konfigurationen, ob ein Datenpaket durchgelassen wird oder nicht.

Stateful Inspection ist die Firewall-Technologie, die den derzeit höchstmöglichen Sicherheitsstandard für Internet-Verbindungen und somit das Firmennetz bietet. Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen verhindert diese Funktionalität den unbefugten Zugriff auf Daten und Ressourcen im zentralen Datennetz. Zum anderen überwacht sie als Kontrollinstanz den jeweiligen Status aller bestehenden Internet-Verbindungen. Die Stateful Inspection Firewall erkennt darüber hinaus, ob eine Verbindung “Tochterverbindungen” geöffnet hat – wie beispielsweise bei FTP oder Netmeeting – deren Pakete ebenfalls weitergeleitet werden müssen. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf. Alternative Bezeichnungen für Stateful Inspection sind: Stateful Packet Filter, Dynamic Packet Filter, Smart Filtering, Adaptive Screening.

Stateful Inspection vereinigt konzeptionell die Schutzmöglichkeiten von Packet Filter und Application Level Gateways d.h. sie integriert als Hybrid die Funktionen beider Security-Verfahren und arbeitet sowohl auf der Netz- als auch Anwenderschicht. Bei der “zustandsabhängigen Paket-Filterung” werden nicht nur die Internet- und Transportschicht sondern auch Abhängigkeiten vom Zustand einer Verbindung berücksichtigt. Alle aktuellen und initiierten Verbindungen werden mit Adresse und zugeordnetem Port in einer dynamischen Verbindungstabelle hinterlegt. Der Stateful Inspection-Filter entscheidet anhand festgelegter Raster (Informationen), welche Pakete zu welcher Verbindung gehören. Zustände können sein: Verbindungsaufbau, Übertragung, Verbindungsabbau und gelten sowohl für TCP- als auch UDP-Verbindungen. Ein Beispiel an einer Telnet-Sitzung: Der Zustand “Verbindungsaufbau” wird dadurch definiert, dass noch keine Benutzer-Authentisierung stattgefunden hat. Hat der Benutzer sich mit Benutzername und Kennwort angemeldet, wird diese Verbindung in den Zustand “normale Verbindung” gesetzt. Da der jeweilige Status einer Verbindung ständig überwacht wird, bleibt Unbefugten der Zugriff auf das interne Unternehmensnetz verwehrt.

Der Vorteil gegenüber statischen Paketfiltern ist, dass die Entscheidung, ob ein NCP Secure Gateway oder Client ein Paket weiterleitet oder nicht, nicht nur auf Grund von Quell- und Zieladresse oder Ports fällt. Das Security-Management prüft darüber hinaus

den Zustand (state) der Verbindung zu einem Partner. Weitergeleitet werden ausschließlich die Pakete, die zu einer aktiven Verbindung gehören. Datenpakete, die sich keiner etablierten Verbindung zuordnen lassen, werden verworfen und im Log-File protokolliert. Neue Verbindungen lassen sich nur entsprechend der konfigurierten Regeln öffnen.

In der einfachsten Firewall-Funktion werden nur die ein- und ausgehenden Verbindungen im Hinblick auf das Protokoll (TCP/IP, UDP/IP, ICMP, IPX/SPX), die entsprechenden Ports und die beteiligten Rechner überprüft und überwacht. Verbindungen werden in Abhängigkeit eines festgelegten Regelwerkes erlaubt oder gesperrt. Weitere Prüfungen (z.B. Inhalt der übertragenen Daten) finden nicht statt.

Die Stateful Inspection Filter sind eine Weiterentwicklung der dynamischen Packet-Filter und bieten eine komplexere Logik. Die Firewall prüft, ob eine am Portfilter erlaubte Verbindung auch zu dem definierten Zweck aufgebaut wird.

Es werden folgende zusätzliche Informationen zu einer Verbindung verwaltet:

- Nr. zur Identifizierung einer Verbindung
- Zustand der Verbindung (z.B. Aufbau, Datenübertragung, Abbau)
- Quell-Adresse des ersten Pakets
- Ziel-Adresse des ersten Pakets
- Interface, durch welches das erste Paket kam
- Interface, durch welches das erste Paket verschickt wurde

Anhand dieser Informationen kann der Filter entscheiden, welche nachfolgenden Pakete zu welcher Verbindung gehören. So kann ein Stateful Inspection-System auch das UDP-Problem ausschalten. Hintergrund ist die verhältnismäßig leichte Fälschbarkeit von UDP-Paketen z.B. beim UDP-basierten Dienst DNS. Da Stateful Inspection-Filter in der Lage sind, sich die aktuelle Status- und Kontextinformation einer Kommunikationsbeziehung zu merken, ist es erforderlich, dass neben der Quell- und Zieladresse sowie Quell- und Zielpport, auch der DNS-Header im Anfrage-Paket in die Speicherung der Status- und Kontextinformation einbezogen wird. Es erfolgt eine Interpretation auf der Anwendungsschicht.

Beispiel: Eine gehenden Verbindung zum Port 21 eines Rechners ist für einen reinen Portfilter eine FTP-Verbindung. Eine weitere Überprüfung findet nicht statt. Der Stateful Inspection-Filter prüft zusätzlich, ob die über diese Verbindung übertragenen Daten zu einer etablierten FTP-Verbindung gehören. Wenn nicht, wird die Verbindung sofort unterbrochen. Weiter ist ein Stateful Inspection-Filter in der Lage, Regeln in Abhängigkeit von notwendigen Kommunikationsprozessen anzupassen. Wenn z.B. eine abgehende FTP-Verbindung erlaubt ist, so ermöglicht die Firewall auch automatisch die Etablierung des zugehörigen Rückkanals. Die entsprechenden Informationen (Ports) werden aus der Kontrollverbindung herausgelesen.

Ein vorteilhafter Aspekt von Stateful Inspection-Filtern ist die Fähigkeit, die Daten auf allen Protokollebenen (d.h. von Netzwerk- bis Anwendungsebene) zu prüfen. So kann z.B. ein FTP-GET erlaubt, ein FTP-PUT jedoch verboten werden. Ein positiver Effekt der im Vergleich zu konventionellen Paketfiltern erhöhten Eigenintelligenz ist die Op-

tion, einzelne Pakete während einer Kommunikationsbeziehung zu assemblieren und damit erweiterte Möglichkeiten zur Benutzer-Authentisierung zur Anwendung zu bringen. Als Folge der nicht verlässlichen Trennung der Netzwerksegmente sind Stateful Inspection-Filter nicht immun gegen bestimmte auf unteren Protokollebenen stattfindende Angriffe. So z.B. werden fragmentierte Pakete i.d.R. von außen nach innen ohne weitere Prüfung durchgelassen.

Diese Seite ist frei →

Abkürzungen und Begriffe

3DES	TripleDES. Verschlüsselungsstandard mit 112 Bit.
AES	Advanced Encryption Standard. Europäische Entwicklung der belgischen Verschlüsselungsexperten Joan Daemen und Vincent Rijmen ("Rijndael-Algorithmus"). Nachfolger von DES (Data Encryption Standard). Verschlüsselungsalgorithmus, der bis zu 256 Bit Schlüssellänge besitzt. n hoch 256 gilt als Maßeinheit für die mögliche Anzahl der Schlüssel, die mit diesem Algorithmus generiert werden können. Trotz steigender Prozessorgeschwindigkeiten wird erwartet, dass der AES-Algorithmus eine akzeptable Sicherheit für die nächsten 30 Jahre bietet. Wird in VPN- und SSL-Verschlüsselungen bald große Verbreitung finden.
AH	Authentication Header RFC 2402
Asymmetrische Verschlüsselung	(Public-Key-Verfahren) Bei einer asymmetrischen Verschlüsselung besitzt jeder Teilnehmer zwei Schlüssel: einen geheimen, privaten und einen öffentlichen Schlüssel. Beide Schlüssel stehen in einer mathematisch definierten Beziehung zueinander. Der private Schlüssel des Teilnehmer ist streng geheim, der öffentliche Schlüssel für jedermann zugänglich. Das Schlüsselmanagement gestaltet sich auch bei großen Teilnehmerzahlen überschaubar: Zwei Schlüssel pro Teilnehmer – ergibt insgesamt 2.000 Schlüssel, um 1.000 Teilnehmern in allen Sender-Empfänger-Kombinationen die sichere Kommunikation zu ermöglichen. Das bekannteste asymmetrische Verschlüsselungsverfahren ist RSA. Nachteil der asymmetrischen Verfahren: Sie sind rechenintensiv und damit vergleichsweise langsam.

Basisanschluss (So / BRI = Basic Rate Interface)	ISDN-Anschlusstyp mit So-Schnittstelle ("S" für Subscriber Interface: Benutzerschnittstelle), bestehend aus einem D-Kanal (Bandbreite: 16 kBit/s) für die Steuerung und zwei B-Kanälen (Bandbreite jeweils 64 kBit/s) für die Übertragung von Nutzinformationen.
BCP	Bridge Control Protocol
BITS	Bump In The Stack. Art der Implementierung von IPsec.
BITW	Bump In The Wire. Art der Implementierung von IPsec.
Blowfish	Verschlüsselungsstandard mit 128/448 Bit
BRI	Basic Rate Interface (ISDN-Schnittstelle, Basis So) mit 2 B-Kanälen und 1 D-Kanal.
Browser	Der Browser stellt die Anwender-Schnittstelle zum Internet dar. Mit seiner HTTP-Fähigkeit (Hypertext-Transfer-Protokoll) kann er verschiedene Formate (z.B. HTML, GIF, CAD), die für eine multimediale Darstellung der Information benötigt werden, in Sound und Grafik umsetzen.
CA	Certification Authority, auch Trust Center (z.B. D-Trust, ein Gemeinschaftsunternehmen der Bundesdruckerei und Debis). Eine CA stellt mittels PKI-Manager (Software) digital signierte Bestätigungen (Zertifikate) aus und brennt sie auf eine Smartcard (Chipkarte). Eine CA kann ein privater Dienstleister oder eine öffentliche Einrichtung sein. Diese Zertifizierungsstellen bedürfen nicht der Genehmigung durch den Staat. Sie haften für die Richtigkeit der Zertifikate.
CAPI	Common Application Programm Interface. Diese Schnittstelle wird im ISDN als Common ISDN API bezeichnet und entspricht der PCI-Schnittstelle (Programmable Communication Interface). Die Schnittstelle erlaubt den direkten Zugang zum ISDN und den unteren Protokollschichten (Ebene 1-3). Höhere Protokolle (Anwendungen) wie Telex oder Filetransfer können unabhängig von der eingesetzten Hardware-Plattform verwendet werden. Die CAPI gibt es in zwei Versionen, 1.1 und 2.0.

Entsprechend sind auch die ISDN-Anwendungsprogramme programmiert, die entweder auf CAPI 1.1 oder CAPI 2.0 aufsetzen, bzw. die jeweilige CAPI voraussetzen. Eine Hybrid-CAPI gestattet sowohl den Einsatz einer Anwendungs-Software für CAPI 1.1 als auch den von CAPI 2.0-Software. (Siehe Hybrid-CAPI)

CCP	Compression Control Protocol
CHAP	Challenge Handshake Authentication Protocol
CLI	Calling Line Identification (Rufnummern-Identifizierung im Euro-ISDN)
COSO	Charge One Side Only. COSO-Rückruf, auch Low Level- oder D-Kanal Rückruf. Für den Initiator des Rückrufs im D-Kanal fallen keine Gebühren an.
CTAPI	Schnittstelle zu Smartcard Readern
CUG	Closed User Group (geschlossene Benutzergruppe im Euro-ISDN)
DES	Datenverschlüsselungsnorm, Data Encryption Standard
DHCP	Mit DHCP (Dynamic Host Control Protocol) zu kommunizieren, bedeutet, dass für jede Session automatisch eine IP-Adresse zugewiesen wird.
Directory Service	Remote Access-Zugänge werden wie E-Mail-Adressen, Telefonnummern etc. in Verzeichnissen auf unterschiedlichen Datenbanken abgelegt. Das Problem bei dieser Vielzahl von Verzeichnissen ist, dass einerseits viele Daten mehrfach erfasst werden und zudem die einzelnen Einträge nicht untereinander verknüpft sind. Der Pflegeaufwand ist enorm und Inkonsistenzen sind nicht auszuschließen. Gefordert ist ein standardisiertes Prozedere, mit Hilfe dessen die Erfassung und Pflege aller Informationen in einer zentralen Directory ermöglicht wird. Das T-Online Security Management unterstützt die standardisierten Protokolle Radius (Remote Authorization Dial In User Service) und LDAP (Lightweight Directory Access Protocol), wobei letztere den Zugriff auf zentralisierte Verzeichnisdienste gewährleistet.

DMZ	Demilitarisierte Zone, zwischen Firewall und Unternehmensnetz, zum Beispiel mit Web-, Email- und VPN-Server.
DNS	Der Domain Name Server (DNS) stellt die IP-Adresse für eine Internet-Sitzung zur Verfügung, nachdem die Anwahl mit Benutzername und Passwort erfolgte. Er routet weiter im Internet, indem er die Namen, die im Browser als gewünschtes Ziel angegeben werden, in IP-Adressen rückübersetzt und die Verbindung zu dieser Adresse herstellt.
D-Kanal-Protokoll	Das D-Kanal-Protokoll sorgt dafür, dass sich Endgeräte mit dem Netz verständigen können. Es steuert unter anderem Verbindungsauf- und abbau. Es umfasst Schicht 2 und 3. Auf Schicht 2 von ISDN ist HDLC für die logische Datenübertragungssteuerung eingesetzt. Das eigentliche D-Kanal-Protokoll ist auf Schicht 3 angesiedelt. Mittlerweile ist DSS1 als europaweites D-Kanal-Protokoll verfügbar.
DSA	Directory System Agent
DSS1	European Digital Subscriber System No. 1. Europäisches ISDN-Protokoll für den D-Kanal.
DUA	Directory User Agent
ECP	Encryption Control Protocol
ESP	Encapsulating Security Payload RFC 2406
Euro-ISDN	ITU-Standard für Europäisches ISDN; bezieht sich auf das D-Kanal-Protokoll DSS1 und mögliche Dienstmerkmale, wie Gebührenanzeige (Advice of Charge), Rückruf bei Besetzt (Completion of Calls to Busy Subscriber), Rufumleitung (Call Forwarding), Anklopfen (Call Waiting), etc. Im Euro-ISDN mit dem D-Kanal-Protokoll DSS1 werden einzelne Endgeräte mit der Multiple Subscriber Number (MSN) adressiert.
Firewall	Trennt Public-Netz von Private-Netz. Schutzmechanismus in Netzen, der den Zugriff der Stationen regelt. Ein Firewall-Rechner schottet ein Netzwerk

vor allem WAN-seitig gegen unautorisierten Zugriff ab. Die Berechtigung kommender und abgehender Verbindungen wird zum Beispiel geregelt durch Herausfiltern bestimmter Netzteilnehmer und Netzdienste und Festlegung der Zugriffsberechtigungen. Vom WAN aus betrachtet stehen hinter der Firewall (in der DMZ) für gewöhnlich Web-Server, Email-Server und VPN-Server.

FTP	File Transfer Protocol. Basiert auf TCP und dem Terminalprotokoll TELNET (Port 21).
GPRS	Standard für schnelle Handy-Kommunikation
GRE	Generic Router Encapsulation. CISO-Spezifisches Tunnel-Protokoll.
GSM	Global System Mobile. Standard für Handy-Kommunikation
Hash-Wert	siehe Signatur
HBCI	Standard für Smartcard Reader (Online Banking)
HTTP	Hypertext Transfer Protocol. Multimedia-Network im Internet (Port 80)
Hybride Verschlüsselung	Hohe Performance plus viel Sicherheit: Hybride Verschlüsselung vereint die Vorteile symmetrischer und asymmetrischer Verfahren. Während die Inhalte der Kommunikation mit schnellen symmetrischen Algorithmen gesichert werden, erfolgen Authentisierung der Teilnehmer und Schlüsselaustausch auf Basis asymmetrischer Verfahren. Die eigentliche Verschlüsselung der Daten eines Dokuments geschieht auf Basis einer Zufallszahl (Session-Key), die für jede einzelne Kommunikationsverbindung neu erzeugt wird. Dieser Einmal-schlüssel wird mit dem öffentlichen Schlüssel des Empfängers chiffriert und der Nachricht beigelegt. Der Empfänger wiederum rekonstruiert mit seinem privaten Schlüssel den Session-Key und entschlüsselt die Nachricht.
IETF	Internet Engineering Task Force. Interessengemeinschaft, die sich mit Problemen des TCP/IP und dem Internet befasst, unter anderem den Well Known Ports (Ports 0 bis 1023).

IKE	Internet Key Exchange. Bestandteil von IPsec für sicheres Schlüssel-Management. Separate security association negotiation and key management protocol RFC 2409
Internet	Das Internet ist ein weltweites, offenes Rechnernetz. Es ist allgemein zugänglich. Jeder Betrieb und jede Privatperson kann sich daran anschließen und mit allen anderen angeschlossenen Benutzern kommunizieren, unabhängig von der eingesetzten Rechnerplattform oder der jeweiligen Netztopologie. Damit der Datenaustausch zwischen den unterschiedlichen Rechnern und Netzen innerhalb des Internets möglich wird, ist ein allen gemeinsames Netzwerkprotokoll nötig. (siehe TCP/IP)
IP-Adresse	Jeder Rechner im Internet besitzt für die Dauer seiner Zugehörigkeit zum Internet eine IP-Adresse (Internet-Protokoll-Adresse), die ihn eindeutig identifiziert. Eine IP-Adresse ist 32 Bits lang und besteht aus vier voneinander durch Punkte getrennte Zahlen. Für jede Zahl stehen 8 Bits zur Verfügung, womit sie 256 Werte annehmen kann. Die Anzahl der möglichen IP-Adressen insgesamt bleibt jedoch begrenzt. Der Internet-User bekommt daher nicht einmalig eine unveränderliche IP-Adresse zugeteilt, sondern für jede seiner Sessions die IP-Adresse, die gerade noch nicht vergeben ist. Die IP-Adressen werden also für die Dauer eines Zeitschlitzes zugeteilt. Diese Adress-Zuteilung erfolgt im Regelfall automatisch per PPP-Verhandlung über DHCP. Die IP-Adresse kann von speziellen Programmen in einen Namen übersetzt werden. Diese Programme laufen auf einem Domain Name Server (DNS).
IP Network Address Translation	(IP Network Address Translation wird bei der Installation der Workstation Software bereits vorgesehen und ist standardmäßig beim Anlegen eines neuen Zielsystems aktiviert!) Wenn IP Network Address Translation verwendet wird, werden alle übertragenen Frames mit der ausgehandelten (PPP) IP-Adresse verschickt. Die Workstation Software übersetzt diese öffentliche IP-Adresse in die systemeigene des Intranets oder, im Falle der Workstation, in deren eigene vom Benutzer festgelegte. Allgemein: Über NAT ist es möglich, in einem LAN mit inoffiziellen IP-Adressen, die nicht im

Internet gültig sind, zu arbeiten und trotzdem vom LAN aus auf das Internet zuzugreifen. Dazu werden die inoffiziellen IP-Adressen von der Software in offizielle IP-Adressen übersetzt. Dies spart zum einen offizielle IP-Adressen, die nicht in unbegrenzter Anzahl zur Verfügung stehen. Zum anderen wird damit ein gewisser Schutz (Firewall) für das LAN aufgebaut.

IPCP

Internet Protocol Control Protocol

IPsec

Standards festgelegt von IETF: RFCs 2401-2412 (12/98)

IPX

Internet Packet Exchange, Netware-Protokoll von Novell

IPXCP

Internetwork Packet Exchange Control Protocol

ISDN

Integrated Services Digital Network. Dienste-integrierendes digitales Fernmeldenetz. Digitales Netz mit Integration aller Schmalband-Kommunikationsdienste (z.B. Fernsprechen, Telex, Telefax, Teletext, Bildschirmtext), bestehend aus Kanälen mit einer Übertragungsgeschwindigkeit von 64.000 bit/s. Ein Basisanschluss im sogenannten Schmalband-ISDN besitzt drei Übertragungskanäle: Kanal B1: 64.000 bit/s Kanal B2: 64.000 bit/s Kanal D: 16.000 bit/s Die Gesamtübertragungsrate beträgt 144.000 bit/s. Dieses Netz soll bis zum Ende dieses Jahrtausends europaweit einheitlich aufgebaut werden. Die Spezifikationen hierfür werden von ITU und CEPT erarbeitet.

ISDN-Adapter

ISDN-Adapter ermöglichen den Anschluss von vorhandenen, nicht ISDN-fähigen Endgeräten an das ISDN. Der Adapter übernimmt dabei die sowohl soft- als auch hardwaremäßige Anpassung der Endgeräteschnittstelle an die ISDN-Schnittstelle (So). Ein ISDN-Adapter mit Upo-Schnittstelle ermöglicht an ISDN TK-Anlagen die Umsetzung der ISDN-Zweidraht-Schnittstelle Upo (Reichweite ca. 3,5km) auf die busfähige ISDN-Vierdraht-Schnittstelle So (Reichweite ca. 150m) nach den Richtlinien der Telekom.

ISP

Internet Service Provider

Kryptographie	Anwendungen sind Verschlüsselung, elektronische Signatur, Authentifikation und Hash-Wert-Berechnung. Mathematische Verfahren, die mit Schlüssel verwendet werden.
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol, siehe Directory Service
MAC-Adresse	Medium Access Control Layer-Adresse. Physikalische Adresse im Netzwerk.
MIB	Management Information Base. Beschreibt die Struktur der Managementinformationen beim SNMP.
MD5	Message Digest 5. Verfahren zur Bildung eines Hash-Werts
NAS	Network Access System
NetBios	Network Basic Input Output System. Schnittstelle, die Datagramm- und streamorientierte Kommunikation bietet.
OCSP	Online Certificate Status Protocol. Wird als Protokoll für die Online-Prüfung von Zertifikaten verwendet.
OSI-Referenzmodell	Von der ISO standardisiertes Modell, das Kommunikation in sieben Schichten beschreibt: 7. Anwendungsschicht (application layer), 6. Darstellungsschicht (presentation layer), 5. Steuerungsschicht (session layer), 4. Transportschicht (transport layer), 3. Netzwerkschicht (network layer), 2. Datenverbindungsschicht (data link layer), 1. physikalische Schicht (physical layer). Die im Netz zu übermittelnden Daten durchlaufen auf der Senderseite die Schichten von 7 – 1, auf der Empfängerseite in umgekehrter Reihenfolge.
PAP	Password Authentication Protocol. Sicherungsmechanismus innerhalb des PPP zur Authentisierung der Gegenstelle. PAP definiert eine Methode, nach dem Aufbau einer Verbindung anhand eines Benutzernamens und eines Passworts die Rechte des Senders zu prüfen. Dabei geht das Passwort im Klartext über die Leitung. Der Empfänger ver-

gleicht die Parameter mit seinen Daten und gibt bei Übereinstimmung die Verbindung frei.

PC/SC

Schnittstelle zu Smartcard Readern

PEM

Ältere Form von Soft-Zertifikaten (ohne Private Key).

Personal Firewall

Die Security-Mechanismen der Client Software vereinigen Tunneling-Verfahren und Personal Firewalling, IP-Network Address Translationen (IP-NAT) sowie universelle Filtermechanismen. Von zentraler Bedeutung ist IP-NAT, denn es sorgt dafür, dass nur vom Rechner ins Internet ausgehende Verbindungen möglich sind. Ankommende Datenpakete werden auf der Basis eines ausgeklügelten Filterings nach genau definierten Eigenschaften überprüft und bei Nichtübereinstimmung abgewiesen. Das heißt: Der Internet-Port des jeweiligen Rechners wird vollständig getarnt und der Aufbau von unerwünschten Verbindungen unmöglich.

PIN

Personal Identification Number

PKCS

Public Key Cryptography Standard. Verschlüsselungssystem mit öffentlichem Schlüssel.

PKCS#10

Die Form, wie ein Zertifikat vom PKI-Manager an die CA (Certification Authority) übertragen wird. Meist geschieht dies per Http – mit SSL verschlüsselt als Https.

PKCS#11

Basis des Smartcard-Standards

PKCS#12

Soft-Zertifikat. Standard der die Syntax der Dateistruktur beschreibt.

PKCS#15

Pointerbeschreibung: Wo befindet sich was auf der Smartcard.

PKI

(Public Key Infrastructure) Die erforderliche Schlüsselinfrastruktur zur authentischen Verteilung öffentlicher Schlüssel wird PKI genannt. Private und öffentliche Schlüssel werden für asymmetrische Kryptographie verwendet. Transaktionsbezogene Sicherheit erfordert eine eindeutige Partner-Authentisierung mittels Zertifikaten, die von einer

vertrauenswürdigen PKI ausgestellt wurden. Insbesondere für E-Commerce bietet PKI den Rahmen für Vertraulichkeit (Geheimhaltung), Integrität (Fälschungssicherheit), Authentizität (Identitätssicherheit) und Nichtbestreitbarkeit.

PoP	Point of Presence
POP3	Protokoll zum Download von E-Mails. Gegenstück zu SMTP (Port 110)
PPP	Point-to-Point-Protokoll. Übertragungsprotokoll in verbindungsorientierten Netzen.
PPP-Verhandlung	Point-to-Point-Protokoll. In einer PPP-Verhandlung wird die IP-Adresse nach Anwahl an den Provider automatisch übergeben.
PRI	Primary Rate Interface (ISDN-Schnittstelle, Primär-Multiplex S2m) mit 30 B-Kanälen und 2 D-Kanälen.
Radius	Remote Authentication Dial In User Service, siehe Directory Service
RA	Registration Authority. Meist ist die Registrierungsstelle die Stelle, die die Daten für die Beantragung eines Zertifikats entgegen nimmt. Die RA ist auch die Stelle, der der Verlust oder der Verfall eines gültigen Zertifikats gemeldet wird und die eine Widerrufsliste (Revocation List) ungültig gewordener Zertifikate herausgibt.
RAS	Remote Access Services. Firmenspezifische (Microsoft) Einwahlhilfe für Remote Access.
RIP	Routing Information Protocol, auch Routing-Modus
RFC	Request for Comment. Normentwurf, Vornorm, die im Internet diskutiert wird und so lange in der Liste der RFCs gehalten wird, so lange sie sich in der Praxis bewährt. Vorformen der RFCs sind Drafts.
Routing-Tabellen	Router benötigen für die Wegewahl im Netz Informationen über die günstigsten Routen von der Quelle zum Ziel. Mit Hilfe der Routing-Tabellen werden diese Strecken vom Router kalkuliert.

Während beim statischen Routing die Tabellen fest vorgegeben sind, erhält der Router beim dynamischen Routing über Router-Informationsprotokolle (z.B. RIP, NLSP, OSPF) Informationen über das Netz, die zu selbst erlernten Routing-Tabellen zusammengestellt werden und ständig aktualisiert werden.

RSA

Das erste Verfahren, das die Anforderungen an die Public Key-Kryptographie erfüllte. Wurde 1977 von Ron Rivest, Adi Shamier und Leonard Adleman erfunden.

Schnittstelle

(Interface) Festlegung der zwischen zwei Geräten – bei der Datenfernübertragung im allgemeinen zwischen Datenendeinrichtung und Datenübertragungseinrichtung – erforderlichen elektrischen Verbindungsleitungen, der auf diesen herrschenden elektrischen Werten, der zur Funktion erforderlichen Signale sowie der Betriebsweise und Bedeutung dieser Signale. Man unterscheidet nach parallelen und seriellen Interfaces.

SHA

Secure Hash Algorithm, siehe auch Signatur

Signatur

Bei der digitalen Signatur wird mathematisch eine Verknüpfung zwischen Dokument und dem geheimen, persönlichen Signaturschlüssel des Teilnehmers erzeugt. Der Absender des Dokuments generiert eine Prüfsumme (sogenannter Hash-Wert), diese codiert er wiederum mit seinem Geheimschlüssel und erzeugt so einen digitalen Signaturzusatz zur ursprünglichen Nachricht. Der Empfänger des Dokuments kann mit dem öffentlichen Schlüssel des Absenders die Signatur prüfen, indem er seinerseits den Hash-Wert aus der Nachricht bildet und diesen mit der entschlüsselten Signatur vergleicht. Da die Signatur des Absenders unmittelbar in das Dokument eingebunden ist, würde jede spätere Änderung bemerkt. Auch ein Abfangen oder Abhören der Signatur über Lauschangriffe erwies sich als zwecklos: Die digitale Signatur ist nicht nachahmbar, da sie den geheimen, privaten Schlüssel verwendet; eine Ermittlung des geheimen Schlüssels aus der Signatur ist nicht möglich.

Smartcard	Wird die Funktionalität der Smartcard genutzt, so wird nach der CHAP-Authentisierung (User ID und Passwort) die “Erweiterte Authentisierung” (Strong Authentication) mittels der auf Smartcard und Gateway hinterlegten Zertifikate durchgeführt. Auf der Smartcard befinden sich unter anderem das Benutzer-Zertifikat, das Root-Zertifikat und der geheime private Schlüssel. Die Smartcard kann nur mit PIN genutzt werden.
SMTP	Simple Mail Transport Protocol. Internet Standard zur Verteilung elektronischer Post. Ist textorientiert und setzt auf TCP auf (Port 25)
SNA	Systems Network Architecture. Hierarchisch orientiertes Netz zur Steuerung von Terminals und zur Unterstützung des Zugriffs auf Anwendungen in IBM Host-Systemen.
SNMP	Simple Network Management Protocol. Netzwerk-Managementprotokoll auf Basis von UDP/IP.
Source Routing	Möglichkeit, in Token Ring-Netzwerken eine Wegwahl zwischen Bridges zu optimieren. Dabei werden die Wegeinformationen an den Datenblock angehängt mit übertragen. Auf diese Weise liegt auch der Weg für die Bestätigung eindeutig fest.
SPD	Security Policy Database
SSL	Secure Socket Layer. Gemäß dem SSL-Protokoll kann der dynamische Schlüsselaustausch (Dynamic Key Exchange) genutzt werden. SSL, von Netscape entwickelt, ist mittlerweile das Standard-Protokoll für dynamischen Schlüsselaustausch.
SSLCP	Secure Socket Layer Control Protocol
STARCOS	Betriebssystem für Smartcards
Symmetrische Verschlüsselung	Sender und Empfänger verwenden bei der symmetrischen Chiffrierung und Dechiffrierung den gleichen Schlüssel. Symmetrische Algorithmen sind sehr schnell und sehr sicher – dies allerdings nur dann, wenn die Schlüsselübergabe zwischen dem Sender und dem Empfänger ungefährdet erfolgen kann. Gelangt ein Unbefugter in den Besitz des Schlüssels, so kann dieser alle Nachrichten ent-

schlüsseln bzw. sich unter Verwendung des Schlüssels als Absender von Nachrichten ausgeben. Soll bei der symmetrischen Verschlüsselung in größeren Gruppen jeder Teilnehmer nur an ihn adressierte Nachrichten lesen können, so ist für jedes Sender-Empfänger-Paar ein eigener Schlüssel notwendig. Die Folge: ein aufwendiges Schlüsselmanagement. So sind bei 1.000 Teilnehmern bereits 499.500 (!) unterschiedliche Schlüssel erforderlich, um sämtliche Wechselbeziehungen zu unterstützen. Bekannteste symmetrische Verschlüsselung ist heute der DES-Algorithmus.

TCP/IP

Transmission Control Protocol / Internet Protocol. TCP/IP ist ein Netzwerkprotokoll für heterogene Netze und an kein Transportmedium gebunden. Es kann auf X.25, Token Ring oder einfach auf die serielle Schnittstelle aufsetzen und eignet sich deshalb besonders als Kommunikationsprotokoll für unterschiedliche (Netz-) Topologien und Rechner-Plattformen, wie sie im Internet gekoppelt sind. Dabei wird jeder Rechner im Netzwerk Internet durch seine IP-Adresse identifiziert. TCP/IP umfasst außerdem vier Internet-Standardfunktionen: 1. FTP: File Transfer Protocol für den Dateitransfer von einem zum anderen Rechner, 2. SMTP: Simple Mail Transport Protocol für E-Mail, 3. TELNET: Teletype Network für Terminalemulation, 4. RLOGIN: Remote Login zur Rechnerfernbedienung

TECOS

Betriebssystem für Smartcards (Versionen 1.2, 2.0)

Token Ring

Netzwerktopologie mit Ringstruktur von IBM.

UDP

User Data Protocol. Baut direkt auf dem darunter liegenden Internet Protokoll auf. Wurde definiert, um auch Anwendungsprozessen die direkte Möglichkeit zu geben, Datagramme zu versenden. UDP liefert über die Leistungen von IP hinaus lediglich eine Portnummer und eine Prüfsumme der Daten. Durch das Fehlen des Overheads mit Quittungen und Sicherungen ist es besonders schnell und effizient.

UMTS	Universal Mobile Telecommunications Service. Künftiger Standard für schnelle Handy-Kommunikation.
VPN	Virtual Private Network. Ein VPN kann als virtuelles Netz grundsätzlich über alle IP-Trägernetze – also auch das Internet – eingerichtet werden. Für die Realisation haben sich zwei Spezifikationen herauskristallisiert: L2F (Layer 2 Forwarding) und L2TP (Layer 2 Tunneling Protocol). Beide Verfahren dienen dazu, einen Tunnel aufzubauen, den man als eine Art “virtuelle Standleitung” bezeichnen kann. Über eine solche logische Verbindung lassen sich neben IP-Frames auch IPX-, SNA- und NetBIOS-Daten transparent übertragen. Am Tunnelende müssen die Datenpakete interpretiert und zu einem Datenstrom auf der Basis des verwendeten Protokolls umgewandelt werden.
WAP	Wireless Application Protocol. Entwicklung von Nokia, Ericson und Motorola.
X.509 v3	Standard Zertifizierung
Zertifikate	Zertificate (Certificates) werden von einer CA (Certification Authority) mittels PKI-Manager (Software) ausgestellt und auf eine Smartcard (Chipkarte) gebrannt. Diese Smartcard enthält u.a. mit den Zertifikaten digitale Signaturen, die ihr den Status eines digitalen Personalausweises verleihen.

Index

802.1x 98

A

Advanced Encryption Standard 203
 AES 54, 153
 AES-128, AES-192, AES-256 190
 Aggressive Mode 150, 188
 AH 184
 Aktivierungsschlüssel 37
 Alternative Rufnummern 138
 Amtsholung 89, 138
 Anschluss 142
 Anschluss (Modem) 142
 APN 143
 Asymmetrische Verschlüsselung 203
 Aussteller (CA) 56
 Austausch-Modus 188
 Authentication Header 184
 Authentisierung | IKE-Richtlinie 153
 Authentisierung am VPN Gateway 47
 authorityKeyIdentifier 58, 60, 197
 Automatische Erkennung der bekannten Netze 81
 automatische Medienerkennung 46, 55, 89, 134
 Automatischer Modus 150
 automatischer Verbindungsaufbau 171
 Autostart 109
 Autostarttyp manuell 196

B

Baudrate 142
 Beenden des Monitors 176
 Benutzername 137, 173
 Benutzername (XAUTH) 158, 159, 174
 Benutzername | HTTP-Anmeldung 140
 Betriebssystem 22
 Blowfish 54, 153
 Bluetooth 22

C

CA (Certification Authority) 56
 CA-Zertifikat 58
 CDP (Certificate Distribution Point) 60
 Certification Authority 204
 Chipkartenleser 44, 91
 Client Logon 172
 Com Port 142
 Com Port freigeben 142
 connect.bat 97

D

Datendurchsatz 54
 Demilitarisierte Zone 206
 DFÜ-Dialer 135, 170
 DH-Gruppe | IKE-Richtlinie 153
 DHCP 31
 Dial Prefix 143
 Dienst zur Erkennung der bekannten Netze 81
 Diesen Telefonbucheintrag nach jedem Neustart 135

Diffie-Hellman	190
Directory Service	205
disconnect.bat	97
DNS	206
DNS-Server	161
Domain Name	161
Domänen-Anmeldung	172
DPD (Dead Peer Detection)	156, 161, 194
Dynamische Linkzuschaltung	146

E

EAP MP5	98
EAP-Authentisierung	44, 147
EAP-Authentisierung vor Zielauswahl durchführen	101
EAP-Optionen	98, 147
EAP-Status	44
Einwahl am VPN Gateway	47
Encapsulating Security Payload	184
End to Site VPN	183
ESP	154, 184
ESP - 3DES - MD5	150
Exch. Mode	150
Extended Authentication (XAUTH)	47, 158, 174, 192
extendedKeyUsage	58, 60
externer Dialer	133

F

Fingerprint	56, 81
Fingerprint des Aussteller-Zertifikats	166
Firewall	206
Firewall, Firewall-Regeln	73
Firewall, Grundeinstellungen	72
Firewall-Einstellungen	70, 185
Firewall-Regel, Anwendungen	79
Firewall-Regel, Bekannte Netze	80
Friendly Net Detection	45
Friendly Net Detection Server (FNDS)	81
Friendly Nets	80

G

Gateway (IPSec)	149
Globale Firewall	45
GPRS	22, 132
GPRS / UMTS aktivieren	52
GSM	22
Gültigkeitsdauer	56

H

Hash IKE-Richtlinie	153
Hayes-Befehlssatz	22
HotSpot	104
HotSpot-Anmeldung	50
HotSpot-Konfiguration	104
HSCSD	22
HTTP Authentisierungs-Script HTTP-Anmeldung	140
HTTP-Anmeldung	139, 147
HTTP-Authentisierung	140, 147
Hybride Verschlüsselung	207

I

ID Identität	158
Identity Protection Mode	188

IKE	183
IKE (IPSec)	55
IKE Config Mode verwenden	161
IKE ID-Typ	195
IKE-Config Mode	194
IKE-Modus	188
IKE-Richtlinie	149, 152, 186, 188
Internet Key Exchange	183, 188
IP Network Address Translation	208
IP-Adresse manuell vergeben	161, 195
IP-Adressen-Zuweisung	160
IP-Kompression	47
IP-Netzmaske	180, 181, 182
IPCOMP (LZS)	191
IPSec	183
IPSec-Einstellungen	148
IPSec-Kompression	54
IPSec-Maschine	183
IPSec-Richtlinie	150, 186
IPSec-Richtlinienagent	196
IPSec-Tunneling	158, 161
IR-Schnittstelle (Infrarot)	22
ISDN	131, 146

K

Kommunikation im Tunnel	170
Kompression	47
Konfigurations-Sperren	102
Kontrollkanal	187

L

LAN (over IP)	132
LAN IP-Adresse	179
LAN-Adapter schützen	199
Layer-3-Tunneling	183
Limit-Überschreitung	97
Line Management	144
Link Firewall	45, 70
Lizenz-Update	117, 123
Lizenzierung	27
Lizenzinfo und Aktivierung	27
Log-Einträge	105
Logon Optionen, NT	99
Lokale IP-Adresse verwenden	161, 195
lokale Netze im Tunnel weiterleiten	163
Lokales System	27
LZS	54, 156

M

Main Mode	150, 188
Major Release	125
manueller Verbindungsaufbau	171
MD5	44, 81, 153, 154, 191
Meldungen des ACE-Servers für RSA-Token	62
Modem	131, 141
Modem Init. String	143
Multifunktionskarte	43, 51

N

Name IKE-Richtlinie	153
Name IPSec-Richtlinie	154
NAS-Einwahl	46

NAT Traversal	161, 196
NAT-T (NAT Traversal)	194
ncpphone.cfg	34
NCPPI.CONF	26
NetBIOS über IP zulassen	170
netstat	196
Netzeinwahl	136
Netzstatus	196
Netzsuche	51
Netzwerk-Adressen VPN IP-Netze	163

P

Passwort	137, 173, 176
Passwort (XAUTH)	158, 159, 174
Passwort HTTP-Anmeldung	140
Passwort für VPN-Einwahl	174
Passwort speichern	137
Passwort speichern HTTP-Anmeldung	140
Passwörter und Benutzernamen	173
Personal Firewall	45
PFS (Perfect Forward Secrecy)	191
PFS-Gruppe	150
PIN ändern	62, 63
PIN-Abfrage	94
PIN-Benutzung	62
PIN-Eingabezwang	62
PIN-Richtlinie	95
PIN-Status	45, 62
PKCS#12-Datei	91
PKCS#12-Dateiname	93
Policies	186
PPTP	132
Pre-shared Key	47, 149, 158, 193, 194
Profil für automatische Medienerkennung	134
Profil-Einstellungen	67, 128
Profil-Name	131
Profil-Sicherung	103
Protokoll IPSec-Richtlinie	154
PSec-Richtlinie	154
PSK (Preshared Key)	190
PUK Eingabe	53

R

Revocation List	198
RFC 2401	183
RFC 2401 - 2409	183
RFC 2409	183
Richtlinien	186
RSA Signatur	194
RSA-Signatur	149, 188, 189
Rückrufmodus	138
Rufnummer (Ziel)	137
Rx	146

S

SA	184
SA-Verhandlung	186, 187
Schwellwert für Linkzuschaltung	146
Script-Datei	138
Seamless re-keying	191
Secure Policy Database	183

Security	183
Security Association	184
Security-Richtlinie	183
Security-Richtlinien	183
Selektor	183
Seriennummer	37, 56
Service Release	125
SHA	153
SHA-1	191
SHA-1 Fingerprint verwenden	166
Shared Secret	158
SIM PIN	143
SIM PIN ändern	52
Site to Site VPN	183
Smart Card-Symbol	61
Software-Update	125
Source Routing	214
SPD Entry	183
Sperre aufheben	97
Sperrlisten	198
Split Tunneling	162
SSL-Server-Authentisierung	60, 198
Stateful Inspection	199
Stateful Inspection aktivieren	170
Static Key	55
Statistik	53
Statistik (Verbindungssteuerung)	64
Statusanzeigen	44, 46
subjectKeyIdentifier	58, 60, 197
Subnet-Masken	163
Symmetrische Verschlüsselung	214

T

Telefonbuch	34, 36
Timeout	54, 145, 175
TLS	44, 81
Token (PKCS#11)	26
Transformation (Comp)	154
Transformation (ESP)	154
Transportmodus	184
Treibersignatur	27
Trennen	175
Triple DES	54, 153
Tunnelmodus	184
TxRx	146
Typ Identität	158

U

Übertragungstechnik	52
UDP Port 500	196
UDP Pre-Filtering	83
UDP-Encapsulation	156
UMTS	132, 143
Update	125
Update-Key	125

V

Verbinden	171
Verbindungs-Informationen	53
Verbindungsabbau bei gezogener Chipkarte	94
Verbindungsabbruch	175

Verbindungsaufbau	145, 171
Verbindungsmedium	54, 131
Verbindungstyp	131
Verbindungszeit	54
Verschlüsselung	47
Verschlüsselung IKE-Richtlinie	153
Virtual Private Network	216
VPN-Einwahl	46

W

wechselnde Verbindungsart	134
wechselnder Verbindungsaufbau	171
Windows Logon	99, 172
WINS-Server	161
WLAN unter Windows 2000/XP	133
WLAN unter Windows 98/NT	133
WLAN-Automatik	85

X

XAUTH	158, 194
xDSL (AVM - PPP over CAPI)	132
xDSL (PPPoE)	132

Z

Zertifikats-Erweiterungen (Extensions)	58
Zertifikats-Konfiguration	91
Zertifikats-Überprüfung	164
Zertifikats-Überprüfungen	197
Zertifikatsverlängerung	95
Zieladresse des VPN-Gateways	47
Zugangsdaten	159

Anhang zu
NCP Secure Enterprise Client und NCP Secure Entry Client:

Mobile Computing via GPRS/UMTS und Domänenanmeldung mit NCP Gina



Network
Communications
Products engineering GmbH

Dombühler Str.2
D-90449 Nürnberg
Tel.: 0911 / 99 68-0
Fax: 0911 / 99 68-299
internet [http:// www.ncp.de](http://www.ncp.de)

Inhalt

1. Mobile Computing via “GPRS/UMTS”	A5
1.1 Installation	A6
1.2 Installation des Treibers	A6
2. Konfiguration eines Zielsystems (Profiles)	A8
2.1 Konfiguration mit Assistenten	A8
2.2 Konfiguration im Telefonbuch	A12
3. Der Monitor	A14
4. Domänenanmeldung mit NCP Gina	A17
4.1 Logon-Optionen	A19
5. Log-Dateien	A21

Diese Seite ist frei für Notizen

1. Mobile Computing via “GPRS/UMTS”

Wird eine Multifunktionskarte* für UMTS/GPRS/WLAN eingesetzt, so können mit der NCP Client Software** spezielle Features des Mobile Computings unter Einbeziehung der Karteneigenschaften genutzt werden.

Aufgrund der direkten Unterstützung der Multifunktionskarte für UMTS/GPRS/WLAN durch den Secure Client kann die Installation einer Management-Software von der eingesetzten Karte entfallen.

Der NCP Secure Client vereint alle kommunikations- und sicherheitstechnischen Mechanismen für eine wirtschaftliche Datenkommunikation auf Basis des Ende-zu-Ende Sicherheitsprinzips. Der Client-Monitor verfügt über optische Anzeigen aller Verbindungsstati, der Feldstärke, des selektierten Netzes und Providers. Auch die integrierte dynamische Personal Firewall ist optimiert für Remote Access und schützt den mobilen Telearbeitsplatz bereits bei Systemstart gegen jegliche Angriffe und garantiert ein Maximum an Sicherheit auch während der automatischen Hotspot-Anmeldung. Die VPN-Verbindung wird unabhängig vom Microsoft DFÜ-Netzwerk über den integrierten NCP Dialer aufgebaut.

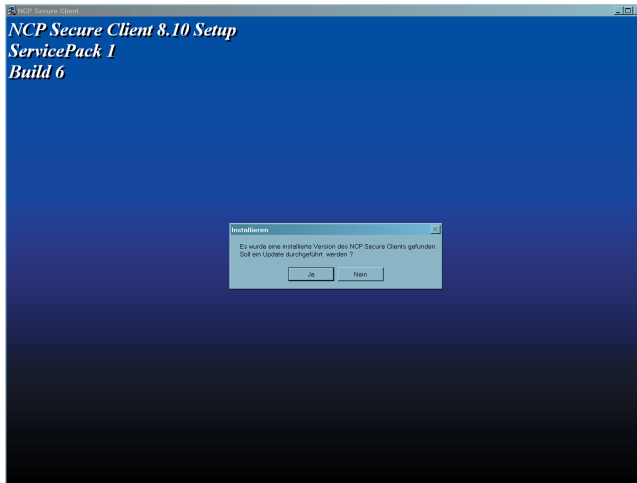
* derzeit unterstützte Multifunktionskarten:

T-Mobile Multimedia NetCard
Vodafone Mobile Connect Card
KPN Mobile Connect Card

** alternative Versionen der NCP Client Software:

Enterprise Client ab Version 8.10 SP1
Entry Client ab Version 8.21

1.1 Installation



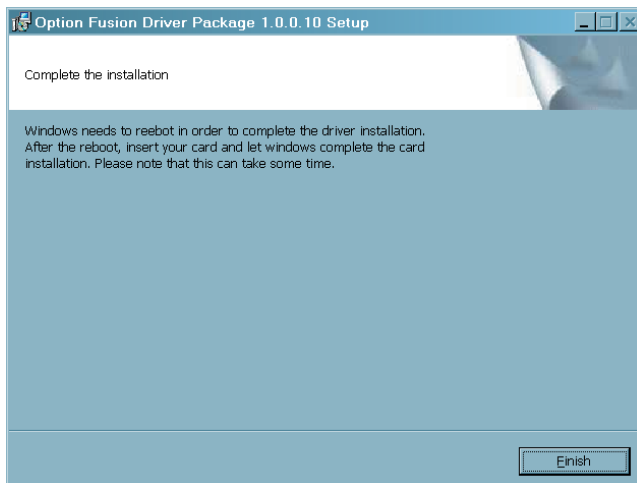
Installieren Sie zunächst die entsprechende Software-Version und spielen Sie anschließend den Treiber der PCMCIA-Karte an Ihrem Notebook ein.

1.2 Installation des Treibers

Der Treiber zur PCMCIA-Karte Qualcomm 3G CDMA befindet sich auf der zugehörigen CD im Verzeichnis

`Software\Modems\Language Independent\`

Starten Sie dort “OptionFusion.exe” mit Doppelklick und bestätigen Sie die daraufhin erscheinenden Fenster mit “OK”.



Nach der erfolgten Komplettierung der Installation, beenden Sie das Setup mit einem Klick auf “Finish”.

Daraufhin wird der Rechner gebootet.

Nachdem Reboot stecken Sie die Karte in einen PCMCIA-Slot.

Bitte beachten Sie bei Einsatz des Betriebssystems Windows XP



Wird Windows XP mit Service Pack 2 und Sicherheits-Packages eingesetzt, so kann eine Verbindung über die Karte nicht hergestellt werden.



Bei einem Verbindungsaufbau zeigt die Software eine Fehlermeldung an (siehe Abbildung links).

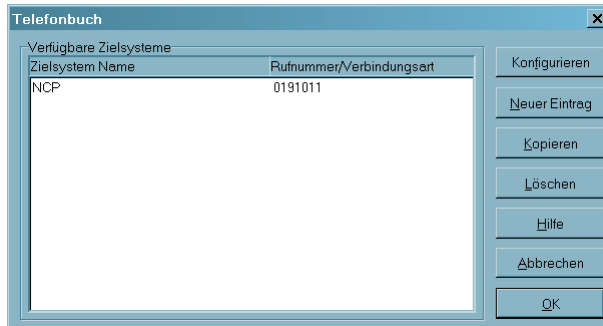
In diesem Fall muss ein neuer Treiber eingespielt werden. Dafür ist die Datei OptionCardInstaller.exe von NCP erhältlich.

Ein entsprechend neuerer Treiber befindet sich auch auf der Treiber-CD zur neueren Multimedia NetCard von T-Mobile, die nur UMTS/GPRS unterstützt.

2. Konfiguration eines Zielsystems (Profiles)

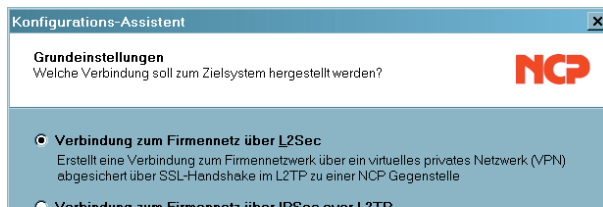
Legen Sie ein neues Zielsystem (Profil) der NCP Client Software an. Beachten Sie dazu die Beschreibung im Handbuch zur Client Software.

2.1 Konfiguration mit Assistenten



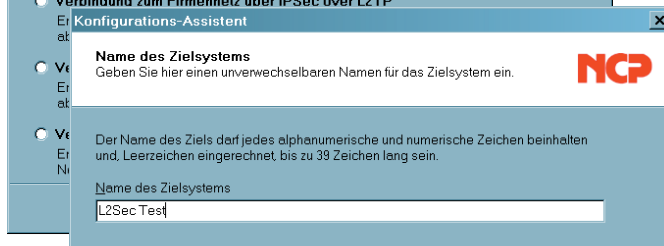
Klicken Sie auf “Neuer Eintrag” und erfüllen Sie die Eingabeaufforderungen des Assistenten. Anschließend kann die Konfiguration im Telefonbuch komplettiert werden.

Im folgenden wird als Beispiel eine Verbindung zum Firmennetz über L2Sec beschrieben.

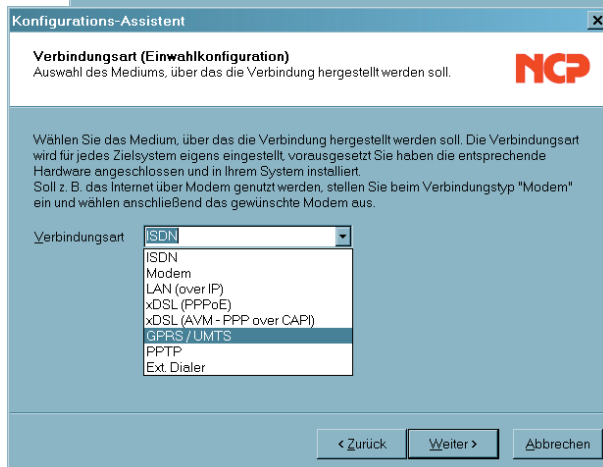


Als Zielsystem dieser Testverbindung dient ein NCP Gateway.

Anschließend auf “Weiter”



Geben Sie für dieses Zielsystem (Profil) einen Namen ein.



Anschließend auf “Weiter”

Als Verbindungsart wählen Sie GPRS/UMTS.

Konfigurations-Assistent

Verbindungsart (Einwahlkonfiguration)
Auswahl des Mediums, über das die Verbindung hergestellt werden soll.

Wählen Sie das Medium, über das die Verbindung hergestellt werden soll. Die Verbindungsart wird für jedes Zielsystem eigens eingestellt, vorausgesetzt Sie haben die entsprechende Hardware angeschlossen und in Ihrem System installiert.
Soll z. B. das Internet über Modem genutzt werden, stellen Sie beim Verbindungstyp "Modem" ein und wählen anschließend das gewünschte Modem aus.

Verbindungsart: **GPRS / UMTS**

Modemauswahl und -einstellungen:

- Agere Systems AC'97 Modem
- Agere Systems AC'97 Modem
- Fusion UMTS GPRS WLAN - 3G Modem**
- AVM ISDN - ISDN (X75)
- AVM ISDN FAX (G3)
- AVM ISDN Custom Config

< Zurück Weiter > Abbrechen

Entsprechend wird in der Modem-Auswahl die Karte "Fusion UMTS GPRS WLAN - 3G Modem" angezeigt. Selectieren Sie diese Karte.

Konfigurations-Assistent

Verbindungsart (Einwahlkonfiguration)
Auswahl des Mediums, über das die Verbindung hergestellt werden soll.

Wählen Sie das Medium, über das die Verbindung hergestellt werden soll. Die Verbindungsart wird für jedes Zielsystem eigens eingestellt, vorausgesetzt Sie haben die entsprechende Hardware angeschlossen und in Ihrem System installiert.
Soll z. B. das Internet über Modem genutzt werden, stellen Sie beim Verbindungstyp "Modem" ein und wählen anschließend das gewünschte Modem aus.

Verbindungsart: **GPRS / UMTS**

Modemauswahl und -einstellungen:

Fusion UMTS GPRS WLAN - 3G Modem

Modem-Initialisierungsstring:
AT&Fcr>ATE0V1&D2&C1S0=0<cr>ATX1<cr>

☐ Impulswahl verwenden

< Zurück Weiter > Abbrechen

Belassen Sie den zugehörigen Modem-Initialisierungsstring unverändert. Schalten Sie die Impulswahl nicht ein.

Konfigurations-Assistent

Zugangsdaten für Internetdienstanbieter
Benutzerinformationen für Internetzugang

Geben Sie hier den Benutzernamen, Passwort und ggfs. die Rufnummer für Ihren Internetdienstanbieter ein. Wollen Sie das Passwort nicht speichern, wird es bei jedem Verbindungsaufbau abgefragt.

Benutzername:
ncpuser12tp

Passwort: Passwort (Wiederholung):

☐ Passwort speichern

Rufnummer Ziel:
*99#

< Zurück Weiter > Abbrechen

Anschließend auf "Weiter"

Als Zugangsdaten für den Internetdienstanbieter (ISP) muss lediglich ein (beliebiger) Benutzername eingegeben werden, es sei denn Sie haben vom Provider spezielle Kennwörter erhalten. Die Abrechnung (und die Identifikation) erfolgt über die SIM-Karte.

Für eine Testverbindung zu einem NCP Gateway tragen Sie als Rufnummer ein:
* 9 9 #

Anschließend auf "Weiter"

Beachten Sie die Beschreibung zu den VPN Gateway-Parametern.

Soll eine Testverbindung zum NCP Gateway hergestellt werden, so geben Sie als Tunnel-Endpunkt ein:
 62.153.165.36
 als Tunnel Secret:
 secret
 Kompression wird nicht benötigt.

Anschließend auf "Weiter"

Für eine Testverbindung zum NCP Gateway ist die Nutzung eines Zertifikats nicht nötig.

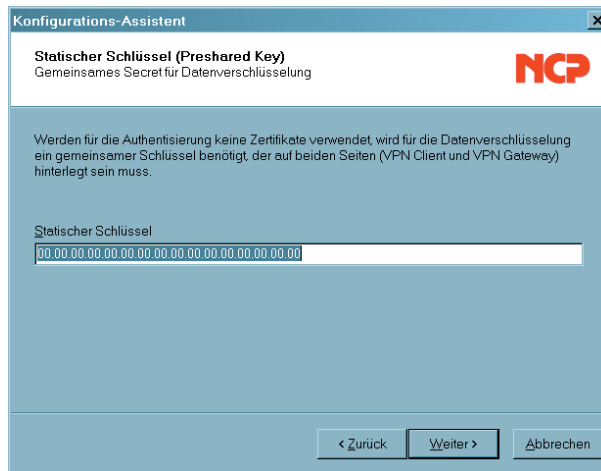
Anschließend auf "Weiter"

Als Zugangsdaten für das NCP VPN Gateway geben Sie folgendes ein:

VPN Benutzername:
 ncpuserl2tp

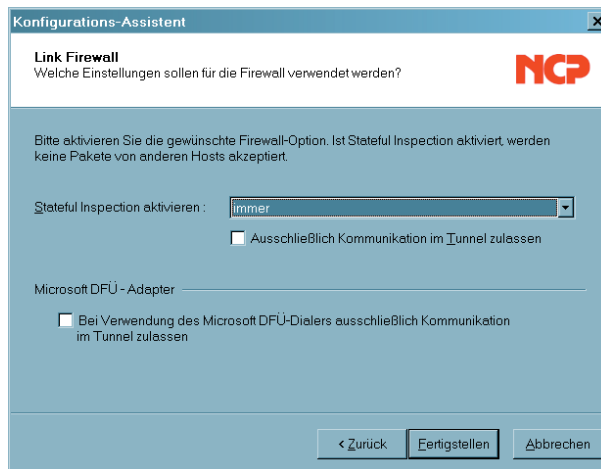
Klicken Sie auf
 "VPN-Passwort speichern" und
 geben Sie als VPN-Passwort
 ein:
 ncpuserl2tp

Anschließend auf "Weiter"



Für die Testverbindung
belassen Sie die Einstellung für
den Statischen Schlüssel.

Anschließend auf “Weiter”



Die Link Firewall muss für die Testverbindung nicht unbedingt gesetzt werden.

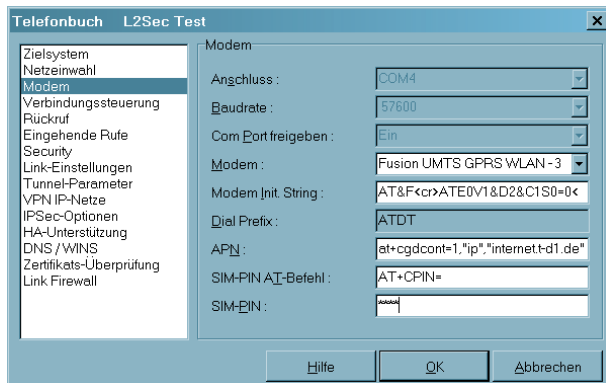
Anschließend auf “Weiter”



Damit ist die Konfiguration mit dem Assistenten abgeschlossen.

Klicken Sie jetzt auf
"Konfigurieren" und
vervollständigen Sie die
Konfiguration im Telefonbuch.

2.2 Konfiguration im Telefonbuch



Selektieren Sie für die Testverbindung das Parameterfeld "Modem" und nehmen Sie folgende Einträge vor:

APN

Der APN (Access Point Name) wird für die GPRS und UMTS-Einwahl benötigt. Sie erhalten ihn von Ihrem Provider. Der APN wird insbesondere zu administrativen Zwecken genutzt.

Der AT-Befehl

```
at+cgdcont=1, "ip",
```

ist Standard für die Übergabe des APN an die SIM-Karte, kann aber je nach Provider variieren.

Der APN

```
"internet.t-d1.de"
```

variiert je nach SIM-Karte und gilt nur für die SIM-D1-Karte von T-Mobile.

SIM PIN AT-Befehl

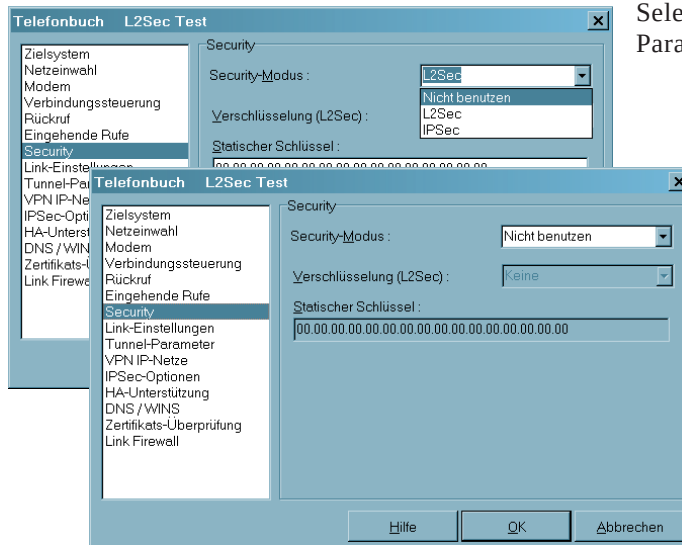
Bei Verwendung einer GPRS/UMTS-Karte muss der jeweils spezifische AT-Befehl eingegeben werden. Dieses Kommando

```
AT+CPIN=
```

ist Standard und bewirkt, dass die SIM PIN richtig erkannt wird.

SIM PIN

Benutzen Sie eine SIM-Einsteckkarte für GPRS oder UMTS, so geben Sie hier die PIN für diese Karte ein. Benutzen Sie ein Handy, so muss diese PIN am Mobiltelefon eingegeben werden.



Selektieren Sie das Parameterfeld “Security”.

Security-Modus

Benutzen Sie für die Testverbindung keinen Security-Modus!

Wählen Sie “Nicht benutzen” und klicken Sie anschließend auf “OK”.

Speichern Sie die Telefonbucheinstellungen und öffnen Sie anschließend den Monitor.

3. Der Monitor



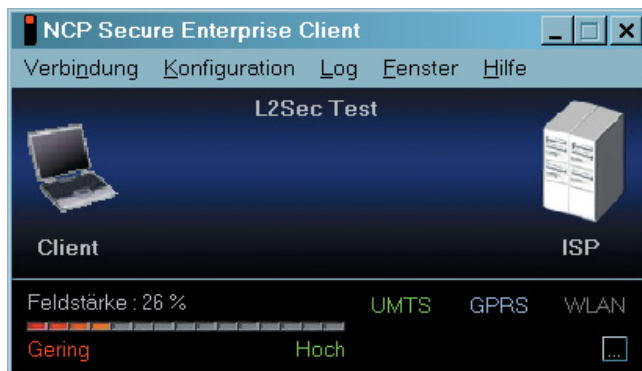
Starten Sie den Monitor.

Der Monitor des VPN/PKI Clients (Enterprise Client) muss sich wie in nebenstehender Abbildung darstellen. Der Monitor des Entry Clients zeigt sich nur unwesentlich anders.

Zwischen dem grafischen Feld und der Button-Leiste muss die Feldstärke des Funknetzes angezeigt werden.

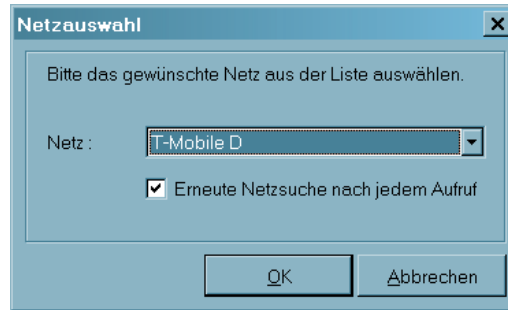


Wird die Feldstärke nicht angezeigt, erscheint eine Fehlermeldung, die auf einen Modemfehler hinweist. Fahren Sie in diesem Fall fort wie unter “1.1 Installation des Treibers” beschrieben wurde!



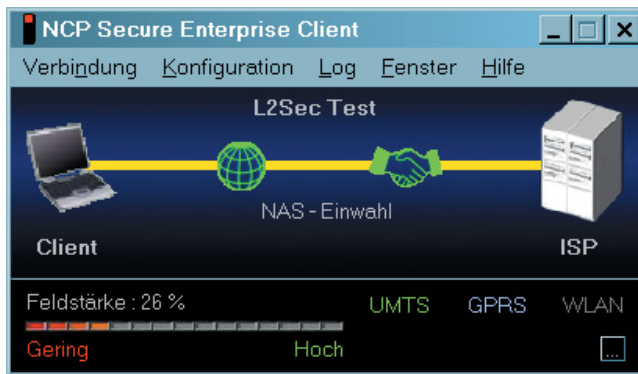
Die Karte sucht nach dem Start des Monitors automatisch nach einem Funknetz und zeigt es mit der entsprechenden Feldstärke an, sobald es gefunden wurde (in der Abbildung links “T-Mobile D”).

Wird das Netz angezeigt, kann durch Klick auf den [...] -Button eine erneute Netzsuche ausgelöst werden.



Nach Netzsuche nach einem alternativen Netz wird das Fenster zur Netzauswahl eingeblendet (links). Das gewünschte Netz kann aus einer Liste ausgewählt werden.

Wird die erneute Netzsuche nach jedem Aufruf des Monitors nicht gewünscht, so muss die standardmäßig aktive Funktion über den Check-Button ausgeschaltet werden.



Der Verbindungsaufbau kann genauso erfolgen wie bei einem Festnetz (vgl. im Handbuch zur Client Software "Verbindungsaufbau"), alternativ mit den Modi "automatisch, manuell oder wechselnd".

Die Verbindungsart wird grün eingefärbt (links "UMTS").



Wenn die Verbindung steht, kann wie im lokalen Firmennetz gearbeitet werden.

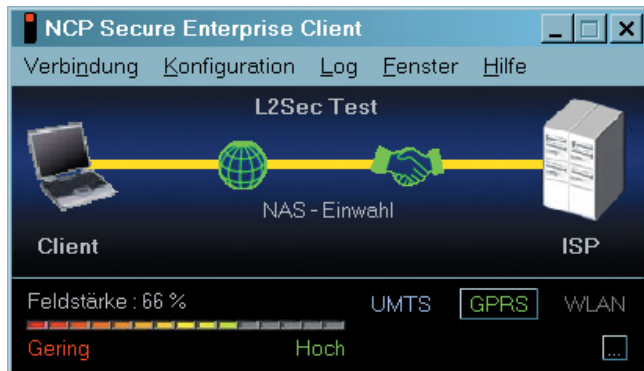
Dies gilt auch für den Fall, dass die Karte bei zu geringer Feldstärke automatisch vom Verbindungsmedium UMTS auf GPRS wechselt. Da in diesem Fall die Verbindung bestehen bleibt.

Erhöht sich die Feldstärke wieder, schaltet die Karte automatisch wieder zurück.



Das Verbindungsmedium kann auch manuell gewechselt werden. Dazu wird mit der Maus das gewünschte Medium angeklickt, im Bild links "GPRS aktivieren".

Bei einem manuellen Wechsel des Mediums wird die Verbindung jedoch zunächst abgebaut.



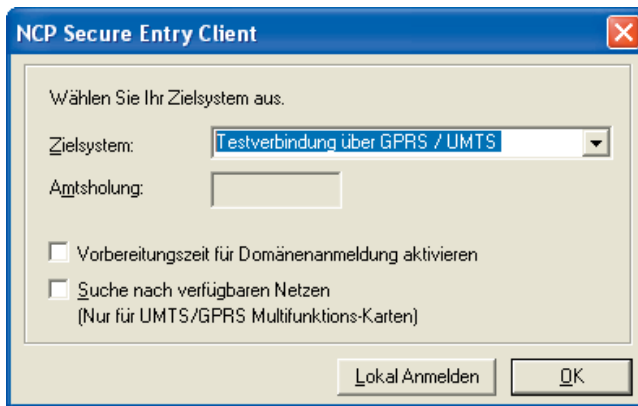
Die Verbindung wird dann wieder automatisch aufgebaut, wenn dies für den Verbindungsaufbau im Telefonbuch konfiguriert wurde.

4. Domänenanmeldung mit NCP Gina



Die Client Software wird bereits in der Boot-Phase im Hintergrund gestartet und fängt den Call “Ctrl-Alt-Delete” ab.

Die integrierte Personal Firewall der NCP Software ist zu diesem Zeitpunkt bereits aktiv, sodass der PC bereits geschützt ist.

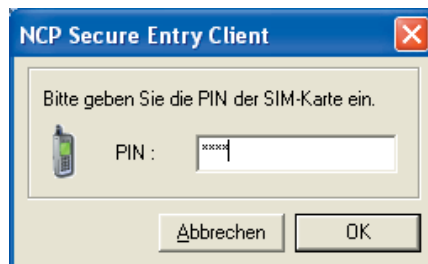


Bereits während der Boot-Phase kann das Zielsystem, das für das Verbindungsmedium GPRS/UMTS konfiguriert wurde, selektiert werden.

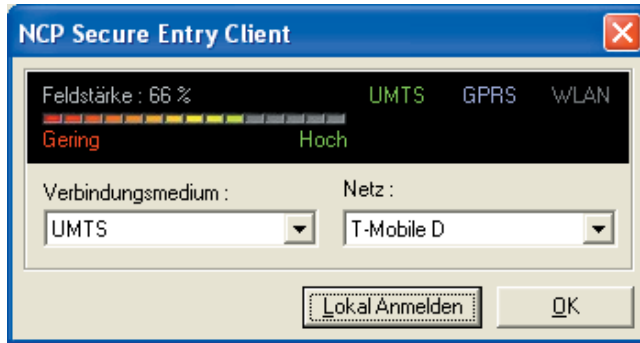
(Die Funktion “Vorbereitungszeit für Domänen-Anmeldung aktivieren” wird nur benötigt, wenn vorher keine ordnungsgemäße Abmeldung erfolgte! Die “Suche nach verfügbaren Netzen” nimmt einige Sekunden in Anspruch und ist in der Regel nur im Ausland von Bedeutung. Vorbereitungszeit für die Domänenanmeldung kann bei Bedarf verlängert werden.)



Bitte beachten Sie zu den möglichen Einstellungen die Beschreibung der Logon-Optionen im Handbuch des Clients!



Die SIM-PIN muss nur dann eingegeben werden, wenn sie in der Konfiguration des Zielsystems (Profils) im Parameterfeld “Modem” im Telefonbuch noch nicht eingegeben wurde oder die abgespeicherte PIN nicht zur aktuell eingesetzten SIM passt.



Anschließend werden die Signale der Karte angezeigt, nach der Netzsuche das gefundene Funknetz mit der jeweiligen Feldstärke.

Wurde die Suche nach alternativen Netzen aktiviert, so kann ein anderes Netz, wie auch ein anderes Verbindungsmedium manuell gewählt werden.

Danach klicken Sie auf "OK", um in der Domänenanmeldung fortzufahren.

(Mit "Lokal Anmelden" brechen Sie den Dialog zur Domänenanmeldung ab.)



Wurde für diese Verbindung die Nutzung eines Zertifikats konfiguriert, muss an dieser Stelle dessen PIN eingegeben werden.

Anschließend klicken Sie auf "OK".



Damit wird die Verbindung hergestellt und ein Tunnel in das Firmennetz der Zentrale hergestellt.

Je nach Konfiguration im Monitormenü unter "Konfiguration / Logon-Optionen" erfolgt das weitere Vorgehen.



1. Der Benutzer gibt wie in der Standard Windows-Anmeldung die gefragten Anmeldeinformationen manuell ein (siehe in der Abbildung unten "Standard Windows-Anmeldung")

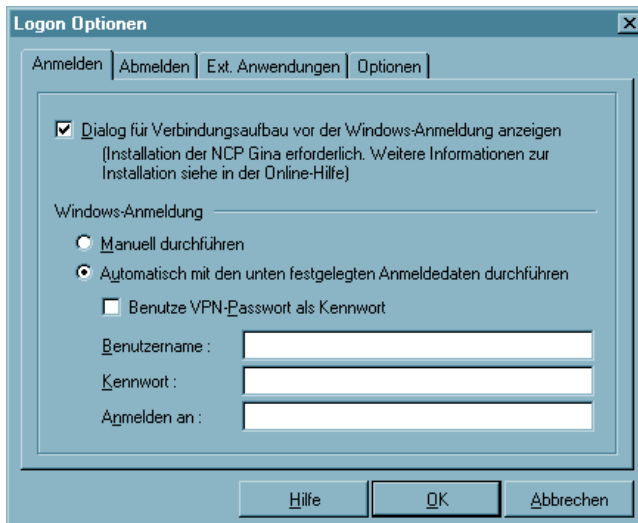
2. Die Client Software übergibt die gefragten Anmeldeinformationen automatisch in diese Maske (der MS-GINA), sodass der Benutzer für das Windows Logon keine Eingaben mehr machen muss. Dazu muss in den Logon-Optionen "Gespeicherte Anmeldeinformationen verwenden" aktiviert sein und die Daten in den Feldern eingetragen sein.

4.1 Logon-Optionen

Die Logon-Optionen werden über das Monitormenü "Konfiguration" selektiert.



Bitte beachten Sie zu den möglichen Einstellungen die ausführliche Beschreibung der Logon-Optionen im Handbuch des Clients!



Anschließend können Sie wählen, ob über den "Dialog für Verbindungsaufbau vor der Windows-Anmeldung" an einer remote Domain die Verbindung von der Client-Software zum Gateway aufgebaut werden soll. Für die Verbindung zum Gateway müssen ggf. die PIN für das Zertifikat, wie auch für die SIM-Karte und das (nicht gespeicherte) Passwort für die Netzeinwahl bereits vor dem Passwort für das Windows Logon eingegeben werden.



Beachten Sie desweiteren:

Aktivieren Sie diesen Dialog nicht, so findet die Passwort- und PIN-Abfrage für das Client Logon erst nach dem Windows Logon statt.

Findet der Verbindungsaufbau vor dem Windows Logon statt, erfolgt die Anmeldung an der remote Domäne bereits verschlüsselt.

Wenn Sie die Logon-Option mit Rückruf nutzen, muss “Verhandle PPP Callback” aktiviert werden (siehe → “Rückruf”).

Nach jeder Änderung der Logon-Optionen im Monitor muss der Rechner gebootet werden.

Diese Funktion kann nur mit Administratorrechten aktiviert werden!

5. Log-Dateien

Ist eine Multifunktionskarte für UMTS/GPRS installiert, wird eine Log-Datei mit folgenden Spalten ins Log-Verzeichnis des Secure Clients geschrieben:

1. Spalte: Zeit
2. Spalte: Aktuelle Feldstärke
3. Spalte: Durchschnittliche Feldstärke der letzten Minute
4. Spalte: Durchschnittliche Feldstärke der letzten 5 Minuten
5. Spalte: Durchschnittliche Feldstärke der letzten 10 Minuten
6. Spalte: Aktueller Netztyp (UMTS oder GPRS)
7. Spalte: Aktuelles Netz

Alle 10 Sekunden wird ein Eintrag erstellt, jedoch nur alle 5 Minuten die Einträge in die Datei geschrieben.

Für jeden Tag wird eine Log-Datei mit dem Namen "mfc<DATUM>.log" erstellt.

Es werden die Log-Dateien der letzten 7 Tage gespeichert.

Diese Seite ist frei für Notizen

Anhang zu
NCP Secure Enterprise Client und NCP Secure Entry Client:

Dienste und Applikationen des Clients



Network
Communications
Products engineering GmbH

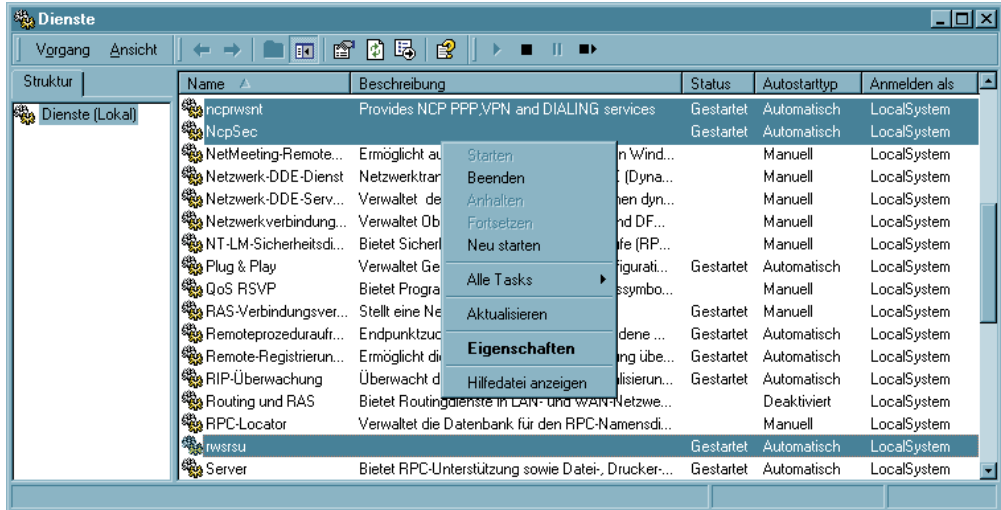
Dombühler Str.2
D-90449 Nürnberg
Tel.: 0911 / 99 68-0
Fax: 0911 / 99 68-299
internet [http:// www.ncp.de](http://www.ncp.de)

Inhalt

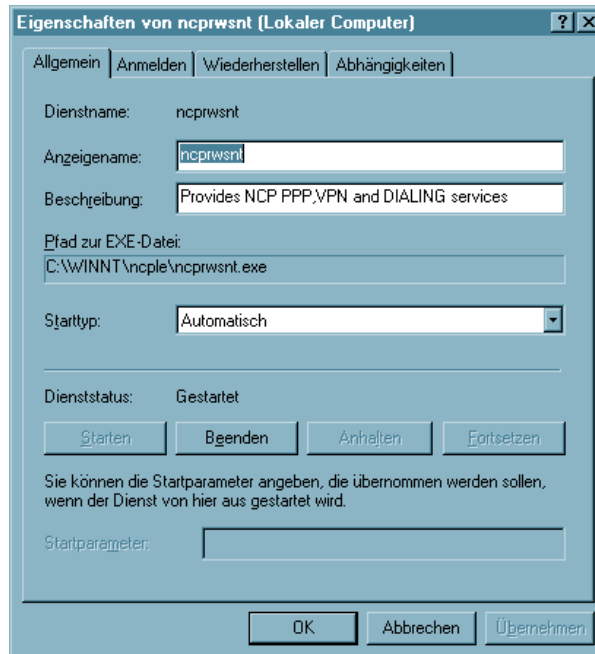
1. Dienste und Applikationen des Secure Clients	A27
1.1 Übersicht der Ports des NCP Secure Clients	A30
bei Win2000/XP:	A30
bei 98/ME:	A30
Weitere Ports:	A30
1.2 Registry-Einträge für den NCP Secure Client	A31
Key: Software\Ncp Engineering GmbH\NCP RWS/GA\6.0	A32
Key: Software\Ncp Engineering GmbH\NCP Secure Client	A32
2. rwsrsu.exe – Update Client	A33
2.1 Funktionsbeschreibung	A33
2.2 Konfiguration	A34
2.2.1 Konfiguration des Update Clients (rwsrsu)	A35
Konfigurationsabgleich durch den Management Server	A35
Update-Intervall (CheckInterval):	A35
Blockgröße (BlockSize):	A35
Weitere Konfigurationseinstellungen in der Registry	A35
2.2.2 Automatisierung der ersten Anmeldung	A37
Beispiel	A37
2.2.3 Konfiguration am Management Servers (ncprsu.exe)	A39
2.2.4 Management Server / Einstellungen	A40
[General]	A40
[Clients]	A44
[Authentication]	A45
[ClientAuthentication]	A46
[CONNMAN]	A47
[CMP]	A47
[RADIUS]	A48
[Log]	A48
[Syslog]	A49
[Console]	A49
2.2.5 Update des Update Clients	A50
3. ncpbudgt.exe – Budget-Manager (Verbindungssteuerung/-statistik)	A51
4. rwscmd.exe – Kommandozeilen-Schnittstelle	A52
4.1 Übergabe von Kommandos an den NCP Secure Client	A52
4.2 Voraussetzung für die Nutzung des Programms	A53
4.3 Beschreibung der Kommandos	A53
5. ncprwsnt.exe	A56
connect.bat	A56
disconnect.bat	A56

1. Dienste und Applikationen des Secure Clients

In der Diensteübersicht des Windows-Systems (im Windows-Startmenü unter “Einstellungen – Systemsteuerung – Verwaltung – Dienste”) können die Dienste ncpsvc.exe, ncprwsnt.exe und rwsrsu.exe aufgesucht werden (Bild unten, Die NCP-Dienste sind in der Abbildung eingefärbt).



Von dieser Windows-Oberfläche können die Eigenschaften der Dienste abgelesen werden (Bild unten), bzw. die Dienste gestoppt oder gestartet werden..

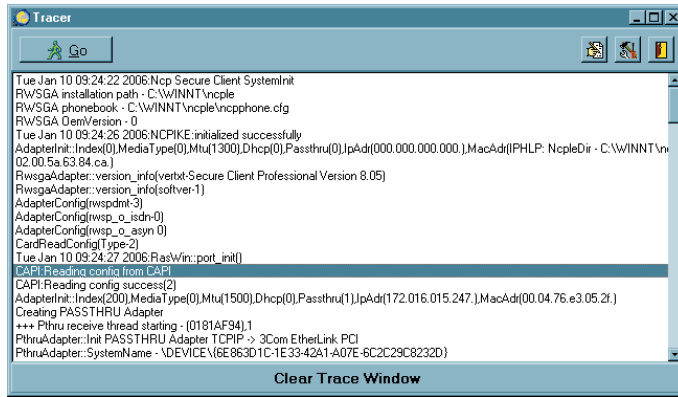


Alle Dienste des Secure Clients werden nach der Installation der Software automatisch aus dem Installationsverzeichnis gestartet.



Zusätzlich zu den Diensten befinden sich außerdem auch Applikationen im Installationsverzeichnis:

ncptrcw.exe



Trace-Monitor; kann auch gestartet werden über “Windows – Programme – Secure Client Tracer”. Dies ist ein eigenes Anwendungsprogramm für qualifizierte Systemtechniker. Mit seiner Hilfe können z.B. Traces zur Fehlersuche erstellt werden. Der Tracer ist nicht für den normalen Benutzer gedacht!

ncpmon.exe

startet den Client-Monitor; kann gestartet werden durch Doppelklick auf das Ampelsymbol in der Task-Leiste oder über “Windows – Programme – Secure Client Monitor”. Die Handhabung und die Menüführung zum Monitor ist ausführlich im Handbuch zum jeweiligen Secure Client beschrieben.

ncpike9x.exe

IKE-Protokoll für Windows 95/98

ncpike.exe

IKE-Protokoll für Windows 2000/XP

lbtrace.exe

Tracer auf Treiberebene für virtuellen NCP-Adapter.

inst95.exe

Installationsprogramm für Windows 95/98

insrnt5.exe

Installationsprogramm für Windows 2000/XP

uninst.exe

Mit diesem Programm kann unter Umgehung der Windows Software-Verwaltung der Secure Client deinstalliert werden.

3monapl.exe

Feldstärkenanzeige für UMTS/GPRS bei Nutzung einer Multifunktionskarte.

ncpauth.exe

dient der Http-Authentisierung

ncprwsnt.exe

Zuständig für das Frame Processing der Datenkommunikation über NCP PPP und VPN, sowie die Wähldienste.

rwsrsu.exe

Update Client; korrespondiert mit dem Programm ncprsu.exe am Management Server, siehe → unten

rwsrsuhlp.exe

Hilfeprogramm für rwsrsu.exe; wird gestartet mit:
`rwsrsu -h`

ncprndll.exe

Wird vom Update Client genutzt und ruft eine DLL auf, die die Dienste des Clients im Update-Fall stoppt bzw. wieder startet.

ncpbudgt.exe

Budget Manager, siehe → unten

ncpmsg.exe

Korrespondiert mit dem Budget Manager und öffnet, sofern im Client-Monitor konfiguriert, das Meldungsfenster mit der entsprechenden Warnung für den Benutzer.

rwscmd.exe

Kommandozeilen-Schnittstelle, siehe → unten

ncppopup.exe

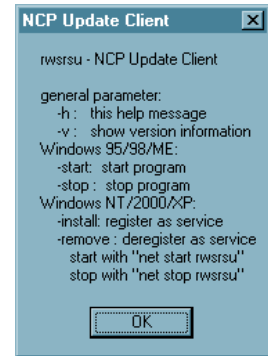
Programm zur Eingabe von Lizenzdaten und Darstellung der Software-Version; kann gestartet werden über “Windows – Programme – Secure Client Popup”.

ncpsec.exe

PKI-Modul der Client Software; dieses Programm wird nur bei Einsatz von digitalen Zertifikaten benötigt. Die Konfiguration von Chipkartenlesern und Soft-Zertifikaten ist ausführlich im Handbuch des jeweiligen Secure Clients im Abschnitt “Monitor” beschrieben.

ncpepsec.exe

Modul für die Endpoint Security zwischen Secure Client und VPN Gateway; die Policies für die Endpoint Security werden am Secure Enterprise Management mit dem Plug-In “Endpoint Policy Enforcement” konfiguriert. Die Erzwingung der Endpoint Sicherheits-Richtlinien (Endpoint Policy Enforcement) ist deshalb nur möglich, wenn das NCP Secure Enterprise Management eingesetzt wird. Nur mit diesem zentralen Management Tool können die Sicherheits-Richtlinien allen Endpunkten der eingesetzten Komponenten gleichermaßen zugeteilt werden. Während die Endpoint Sicherheits-



Richtlinien vom Enterprise Management ausgegeben werden, muss der Download der Sicherheits-Richtlinien (die der Management Server vorschreibt) am VPN Gateway aktiviert werden. Dies erfolgt am Secure Server Manager im Konfigurationszweig "Client Policy Enforcement". Ist die Endpoint Security aktiviert, so erfolgt der Abgleich und der Download der aktuellen Policies über das Programm ncpepsec.exe.



Folgende Dienste und Applikationen sind weiter unten ausführlicher beschrieben:

rwsrsu.exe
ncpbudgt.exe
rwsrmd.exe
ncprwsnt.exe

1.1 Übersicht der Ports des NCP Secure Clients

bei Win2000/XP:

ncpmon.exe	10544
ncpsec.exe	10522, 10542
ncprwsnt.exe	1701, 500, 10523, 10530, 10550, 10600, 10610
rwsrsu.exe	Dynamischer Port nach 12501 (Management Server)

bei 98/ME:

ncpmon.exe	10544
ncpbudgt.exe	10522, 10542
ncpike9x.exe	1701, 500, 10523, 10530, 10550, 10600, 10610
rwsrsu.exe	Dynamischer Port nach 12501 (Management Server)

Weitere Ports:

PKI	10523
PPPoE	10550
IPHlp	10560
WSUP (Driver)	10600
DNS Client	10610

1.2 Registry-Einträge für den NCP Secure Client

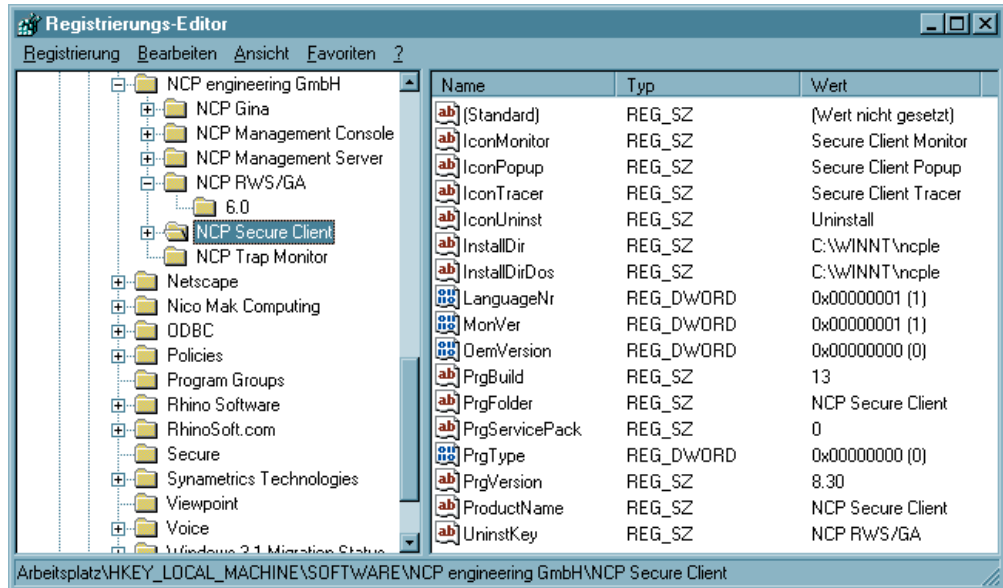
Die Registry-Einträge sind mit dem Registrierungs-Editor unter zwei Verzeichnis-Pfaden zu finden:

Software\Ncp Engineering GmbH\NCP RWS/GA\6.0

und

Software\Ncp Engineering GmbH\NCP Secure Client

(siehe Bild unten)



Key: Software\Ncp Engineering GmbH\NCP RWS/GA\6.0

SeClCsi DWORD
Secure Client Connection state Information

Key: Software\Ncp Engineering GmbH\NCP Secure Client

InstallDir STRING
Installations Verzeichniss

ProductName STRING
Name des Produktes z.B: NCP Secure Client

OemVersion DWORD
0=Ncp,
2=T-Online,
4=Dlink,
5=LanCom,
6=Bintec

DisableRws DWORD
1=Client ist inaktiv,
0=Client ist aktiv

PrgFolder STRING
Name des Startmenues

PrgVersion STRING
Version als String
z.B. 8.01

IconMonitor STRING
Menue Name des Monitors

IconPopup STRING
Menue Name des Popups

IconTracer STRING
Menue Name des Tracers

MonVer DWORD
????

UninstKey STRING
Name für Deinstalltions Key in Registry

2. rwsrsu.exe – Update Client

Der Dienst rwsrsu.exe dient der Kommunikation zwischen Secure Client und Enterprise Management (früher Update Server) und fungiert als Update Client. Mit Hilfe von rwsrsu.exe wird ein automatisches Update von Soft-Zertifikaten, Konfigurationen und Software angestoßen.

2.1 Funktionsbeschreibung

Bei jeder verschlüsselten VPN-Verbindung eines Secure Clients zum NCP Secure Server findet ein automatischer Datenabgleich zwischen Secure Client und Enterprise Management (früher Update Server) statt. (Bei reinen Wählverbindungen ist dieser Update Service nicht nutzbar!)

Ist ein Enterprise Management Server (Update Server) installiert und die entsprechende Konfiguration durchgeführt, schickt der NCP Secure Server (VPN Gateway) nach Authentisierung des Clients die IP-Adresse des Management Servers (Update Servers) zum Client. Wurde der Update Client entsprechend konfiguriert (siehe unten die Registry-Einträge), so wird eine erweiterte Log-Ausgabe erzeugt, in der die IP-Adresse des Management Servers unter dem Eintrag PRIDLS (Primary Download Server) zu finden ist. Ist der NCP Secure Enterprise Management Server hinter einem fremden VPN Gateway installiert, so muss dessen IP-Adresse im Telefonbuch des Secure Clients hinterlegt sein (unter “DNS/WINS – Management Server”).

Im Anschluss daran kontaktiert der Dienst rwsrsu vom Client den Management Server (Update Server), um einen Versionsvergleich vorzunehmen. Dies geschieht mindestens nach jedem Neustart des Secure Clients bei der ersten VPN-Verbindung zum zentralen VPN Gateway.

Sobald der Dienst rwsrsu erkennt, dass eine neuere Version für den Secure Client bereitliegt, wird je nach Konfiguration eine neue Software, eine aktualisierte Konfiguration (Telefonbuch), eine PKCS#12-Datei (Soft-Zertifikat) sowie CA-Zertifikate an den Secure Client übertragen.

Dabei erfolgt das Update eines Telefonbuchs oder eines Zertifikats abhängig von der am Client verwendeten VPN User ID (VPN-Benutzername). Dabei kann unterschieden werden, ob jeder Benutzer ein individuelles Verzeichnis für hinterlegte Konfigurationen erhält oder ob hierfür ein allgemeines Verzeichnis für alle VPN-Benutzer herangezogen werden soll. Letztere Option steht allerdings nur in Verbindung mit Zertifikaten zur Verfügung.

2.2 Konfiguration

Sowohl der Management Server als auch der Update Client (NCP Secure Client) können eigens für die Kommunikation miteinander eingestellt werden.

Werden Konfigurationen vorgenommen, so muss der Dienst bzw. das Programm danach zuerst gestoppt und anschließend erneut gestartet werden, damit die Änderungen wirksam werden:

beim Management Server mit:

```
net stop ncprsu  
net start ncprsu
```

beim Update Client unter Windows NT/XP/2000 mit:

```
net stop rwsrsu  
net start rwsrsu
```

beim Update Client unter Windows 98/ME im Verzeichnis installdir\ncple\ mit:

```
rwsrsu /stop  
rwsrsu /start
```

2.2.1 Konfiguration des Update Clients (rwsrsu)

■ Konfigurationsabgleich durch den Management Server

Der Dienst rwsrsu (Remote Software Update), der am Secure Client immer aktiv ist, wird zunächst vom Management Server eingestellt. Der Update Client erhält dazu das Update-Intervall und die Blockgröße zum Abgleich. Diese Daten werden aus der Konfiguration des Management Servers an den Client bei dessen Logon übertragen.

Update-Intervall (CheckInterval):

Das Update-Intervall ist bei Auslieferung auf einen Tag eingestellt. Mit dem Update-Intervall ist die Zeitspanne in Sekunden festgelegt, nach der der Secure Client, bzw. der Dienst RWSRSU, den Management Server kontaktiert, um zu prüfen, ob aktualisierte Dateien vorliegen.

Blockgröße (BlockSize):

Die Blockgröße bezeichnet die maximale Größe der zu übertragenden Datenpakete in Byte. Sie darf nicht größer als 64 kByte sein.

■ Weitere Konfigurationseinstellungen in der Registry

Weitere Einstellungen für den Update Client können in der Datei ncpmon.ini unter der Rubrik RWSRSU vorgenommen werden:

Registry-Eintrag	Bedeutung
RsuPort	Port für TCP-Verbindung zum Management Server Standard ist 1250 Der Port muss mit dem RsuPort in der Datei NCPRSU.CONF am Management Server übereinstimmen.
RsuLogLevel	Wenn dieser Eintrag existiert, werden erweiterte Log-Ausgaben in der Datei installdir\RWSRSU.LOG erzeugt. Erlaubte Werte sind 0 - 9.
RsuLogFileSize	Maximale Größe der Log-Datei in Byte Standard ist 200.000 Byte

RsuAutoAnswer

Diese Einstellung kann auch geändert werden mit:

...\installdir\rwscmd /rwsautoanswer

Ist dieser Eintrag vorhanden, so kann mit folgenden Werten bestimmt werden wie der Update Client im Falle eines bereitstehenden Software Updates mit der Frage nach dem Update umgeht:

0 = off (standard)

Die Frage, ob ein Update durchgeführt werden soll, wird für den Benutzer sichtbar eingeblendet. Der Benutzer wählt ja oder nein.

1 = yes

Alle Updates werden automatisch durchgeführt, ohne den Benutzer zu fragen.

2 = no

Das Update wird nicht durchgeführt.

2.2.2 Automatisierung der ersten Anmeldung

Die erste Anmeldung (Initialisierungs-Logon) des Clients am Management Server bei einem Rollout kann über Batch-Dateien automatisiert werden. Eingaben des Benutzers, die er aus den Angaben z.B. des PIN-Briefes entnimmt, können auf diese Weise, statt interaktiv, über entsprechende Parameter und Batches an ein Tool übergeben werden. Für diese automatische Init User-Prozedur dient das Programm `rwscmd.exe` (ab Secure Client V.7.21) mit folgenden Kommandos:

```
rwscmd /setinituser <name> [<auth code>]
```

Schreibt die angegebene VPN User ID und den Authentisierungs-Code in die Registry, von wo sie vom Update Client ausgelesen werden.

```
rwscmd /rsuautoanswer <off | yes | no>
```

Vermerkt den gewünschten Modus in der Registry

off = Benutzer fragen, ob ein Software Update durchgeführt werden soll
yes = Software Update immer durchführen
no = kein Software Update durchführen

```
rwscmd /select [Destination Name]
```

Wählt das angegebene Telefonbuch-Ziel aus



Bitte beachten Sie außerdem: Nach einem erfolgreichen Init-Logon überprüft der Update Client ob die Datei `rsuinit.bat` im Installations-Verzeichnis vorhanden ist. Ist dies der Fall, so wird sie automatisch nach dem Disconnect ausgeführt. Zu beachten ist unbedingt, dass innerhalb dieses Batches die vollständige Pfad-angabe (z.B. beim Aufruf von `RWSCMD`) nötig ist, da der Standardpfad nicht das Installations-Verzeichnis ist.

Beispiel

Eine Batch-Datei für die erste Anmeldung mit dem “Mehrfach-Benutzer” muss per Hand gestartet werden und kann so aussehen:

STARTINIT.BAT

```
c:\installdir\rwscmd /setinituser <name> [<auth code>]
c:\installdir\rwscmd /rsuautoanswer yes
c:\installdir\rwscmd /connect [Destination Name]
```

Die RSUINIT.BAT, die genau diesen Namen tragen muss, um automatisch aufgerufen zu werden, kann so aussehen:

RSUINIT.BAT

```
c:\installdir\rwscmd /rsuautoanswer off  
c:\installdir\rwscmd /select [Destination Name]  
c:\installdir\rwscmd /connect  
del c:\installdir\rsuinit.bat
```

Um einen automatisierten nicht-interaktiven InitLogon durchzuführen, müssen folgende Parameter mit rwscmd.exe in die ncpmon.ini geschrieben werden:

Name	Bedeutung
RsuInteractive	= 0 → automatischer InitLogon. In diesem Fall werden die folgenden 2 Werte gelesen.
RsuLogonUserId	zu verwendende VPN User ID
RsuLogonPw	Authentisierungs-Code (nur bei LDAP-Auth. nötig)

2.2.3 Konfiguration am Management Servers (ncprsu.exe)

Die Information, welche IP-Adresse der Management Server hat, erhalten die Update Clients innerhalb der PPP-Verhandlung beim Verbindungsaufbau zum VPN Gateway. Ist der Management Server hinter einem fremden VPN Gateway installiert, so muss dessen IP-Adresse im Telefonbuch des Secure Clients hinterlegt sein (unter "DNS/WINS – Management Server").

Der Rechner mit dem Management Server muss vom NCP Secure Server (VPN Gateway) im Netzwerk per TCP/IP erreichbar sein.

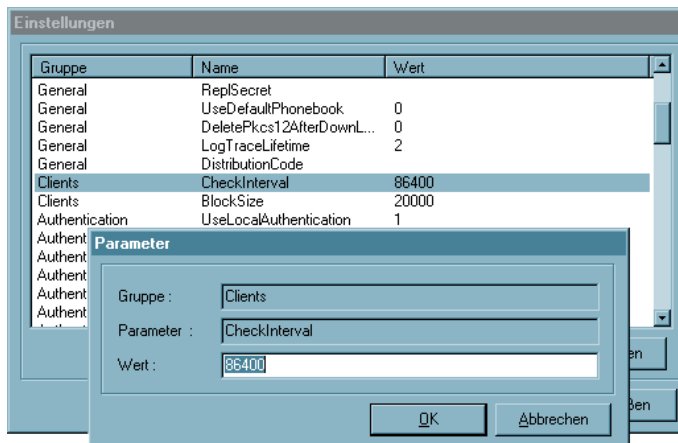
Wird der Management Server auf dem gleichen Rechner wie der Secure Server (VPN Gateway) installiert, so ist darauf zu achten, dass in der Konfiguration mit dem Secure Server Manager die IP-Adresse des Management Servers nicht identisch mit der Adresse des Tunnel-End-Punktes ist, den die Clients zum Aufbau des Tunnels verwenden. Ansonsten würde der rwsrsu-Dienst versuchen, eine Verbindung zum Management Server außerhalb des Tunnels herzustellen, was in der Regel bereits von der Firewall unterbunden wird.



Die weitere Konfiguration des Management Servers erfolgt durch Bearbeitung von Konfigurationsdaten im Hauptmenü der Management Console unter "Management Server / Einstellungen".

2.2.4 Management Server / Einstellungen

In der Management Console öffnen Sie unter dem Hauptmenüpunkt “Management Server” die “Einstellungen”.



Die Parameter sind nach Gruppen geordnet.

Die Werte können nach Doppelklick auf den entsprechenden Parameter geändert werden.



Bitte beachten Sie, dass der Management Server nach einem Editieren der Parameterwerte neu gestartet wird, damit die neue Konfiguration wirksam wird.

[General]

RsuPort = 12501

(Standard = 12501) Muss mit der Einstellung am Update Client (siehe oben → Registry-Eintrag) übereinstimmen.

MgmPort = 12502

(Standard = 12502, sollte nicht verändert werden) Management Port über den der Client Manager die Telefonbücher einstellt.

MgmSSLPort = 12504

(Standard = 12504, sollte nicht verändert werden) Management Port über den der Client Manager die Telefonbücher über SSL einstellt.

ReplPort = 12505

(Standard = 12505, sollte nicht verändert werden) Management Port über den der Management Server ein Backup erstellt.

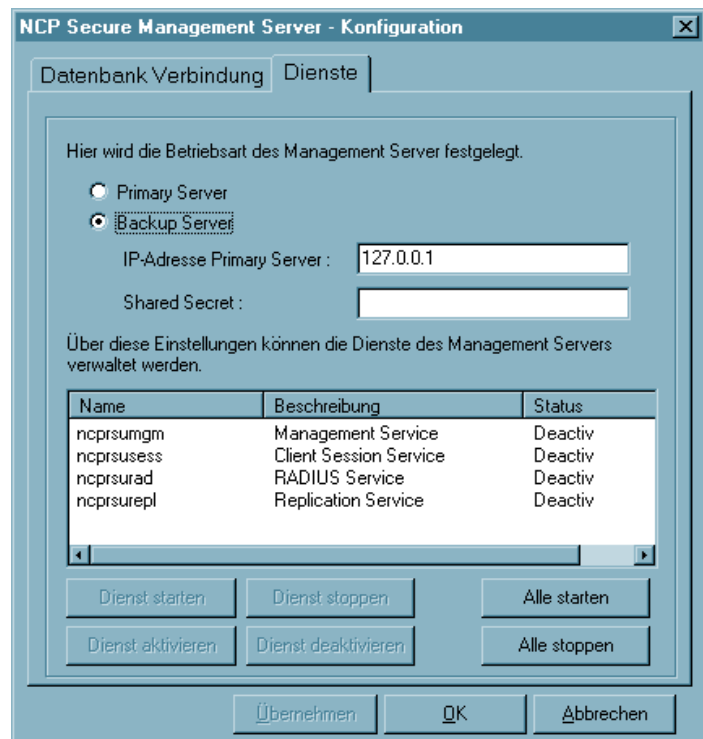
ReplDBPort = 12506

(Standard = 12506, sollte nicht verändert werden) Management Port über den der Management Server die Datenbank repliziert.

MaxSessions = 50

Anzahl der Client Sessions, die der Management Server gleichzeitig abarbeiten soll. Maximal sind 200 Client Sessions möglich.

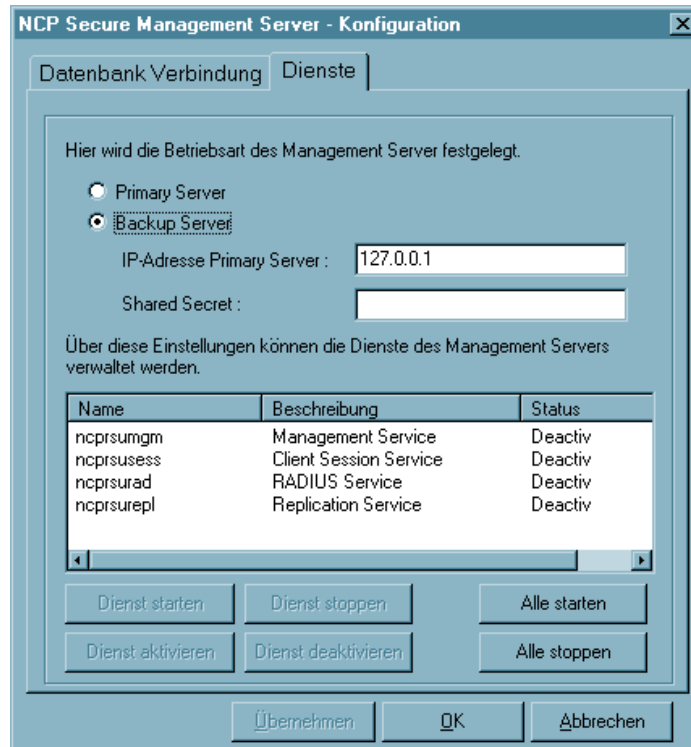
PrimaryIPAddr = 127.0.0.1



Wird der Management Server als Backup Server eingesetzt, so wird hier die IP-Adresse des Primary Servers angegeben. Diese Konfiguration wird vor dem Start des Management Servers im Windows-Startmenü unter "NCP Management Server – Configuration" vorgenommen (siehe Bild oben).

ServerType

= 0



0 = Management Server wird als Primary Server eingesetzt

2 = Management Server wird als Backup Server eingesetzt

Diese Konfiguration wird (unter Windows) vor dem Start des Management Servers im Windows-Startmenü unter "NCP Management Server – Configuration" vorgenommen(siehe Bild oben).

ReplSecret

Wird der Management Server als Backup Server eingesetzt, so wird hier das "Shared Secret" für den Primary Server eingetragen. Diese Konfiguration wird (unter Windows) vor dem Start des Management Servers im Windows-Startmenü unter "NCP Management Server – Configuration" vorgenommen (siehe Bild oben).

DeletePKCS12
AfterDownload

= 0

Standard = 0; nach einem Download wird das Soft-Zertifikat aus der Datenbank gelöscht.

1 = Das Zertifikat wird nicht gelöscht.

LogTraceLifetime	= 2	Anzahl in Tagen bis die Log-Einträge gelöscht werden.
LogLevel	= 9	(mögliche Werte = 0 - 9) Mit dem Wert wird die Tiefe der Analyseebene für die Log-Datei bestimmt.
LogFile	= ncprsu	Der Dateiname der Log-Datei: ncprsu.log
LogPath	= ./log	Das Verzeichnis unterhalb des Installationsverzeichnisses, worin sich die Log-Datei befindet: <Installationsverzeichnis>\log\ncprsu.log
LogFileSize	= 2000000	Dieser Parametereintrag ist optional! Wird die hier in Bytes angegebene Größe der Log-Datei (Standard = 2000000) erreicht, so wird die aktuelle Log-Datei nach <name>.old umbenannt, eine vorherige <name>.old wird gelöscht.
UseDefaultPhonebook	= 0	Durch diesen Schalter für die Telefonbuchauswahl kann festgelegt werden, ob alle Benutzer ein einheitliches Telefonbuch oder jeder ein individuelles vom Management Server zur Verfügung gestellt bekommen. UseDefaultPhonebook = 0 jeder Benutzer erhält sein persönliches Telefonbuch UseDefaultPhonebook = 1 jeder Benutzer erhält dasselbe Telefonbuch
InitUserId	= inituser	Hier wird die Benutzerkennung (User ID) für die erste Anmeldung am Management Server eingetragen. Diese "initiale" User ID für das Rollout ist für alle Clients gleich. Am Secure Server ist daher der Parameter "Erlaube mehrfach Benutzer" für diese Benutzerkennung zu aktivieren. Wählt

sich der Client mit dieser ID ein, so wird vom Management Server die Aufforderung zur Eingabe von persönlichem VPN-Benutzernamen und Passwort/Authentication-Code an den Client zurückgeschickt. Erst nach Eingabe der persönlichen Zugangsdaten kann er ein personalisiertes Telefonbuch bzw. Soft-Zertifikat erhalten.

(Meldet sich ein Client mit dieser InitUserId an und ist keine LDAP-Authentisierung konfiguriert, so wird nur nach seinem VPN-Benutzernamen gefragt. Dabei wird geprüft, ob für diesen eingegebenen VPN-Benutzernamen ein Verzeichnis am Update Server existiert. Ist dies nicht der Fall, so wird die Anmeldung abgewiesen; der Benutzer hat erneut die Chance zur Eingabe einer VPN User ID. Vergleiche Parameter "CheckUserDirAfterInitLogon")

CheckUserDir AfterInitLogon

= 1

Dieser Parametereintrag ist optional! (Standard = 1)

1 = Bei der ersten Anmeldung (InitLogon) ohne Authentisierungs-Code, mit VPN-Benutzernamen wird geprüft, ob für diesen neuen Benutzer ein Verzeichnis existiert. Ist dies nicht der Fall, z.B. bei fehlerhafter Schreibweise des VPN-Benutzernamen, scheitert die Anmeldung und der Benutzer wird zur erneuten Eingabe seines VPN-Benutzernamen aufgefordert.

0 = Die Anmeldung wird dergestalt durchgeführt, dass nach einem Telefonbuch oder einem Soft-Zertifikat für diesen Benutzer gesucht wird. Wird nichts gefunden, so erscheint im Log-Fenster des Benutzer-Monitors: Konfiguration auf dem neuesten Stand.

[Clients]

CheckInterval

= 86400

Das Update-Intervall wird in Sekunden angegeben und ist bei Auslieferung auf einen Tag eingestellt (86400 Sekunden). Das Update-Intervall beschreibt die Zeitspanne, nach der der Secure Client, bzw. der Dienst RWSRSU, den Management Server kontaktiert, um zu prüfen, ob aktualisierte Dateien vorliegen.

BlockSize = 20000

Die Blockgröße bezeichnet die maximale Größe der zu übertragenden Datenpakete in Byte. Sie darf nicht größer als 64 kByte (=65536) sein. Der Update Client gleicht seinen Wert der BlockSize bei jeder Verbindung mit dem Management Server ab.

[Authentication]

Der komplette Konfigurationsabschnitt unter [Authentication] dient dem Rollout, wenn zusätzlich ein LDAP Server zur Verfügung steht.

UseLdapAuthentication = 1

0 = LDAP-Authentisierung wird nicht genutzt

1 = LDAP-Authentisierung wird genutzt

Soll die LDAP-Authentisierung genutzt werden, müssen die folgenden Parameterwerte entsprechend eingesetzt werden. Diese Werte müssen mit jenen übereinstimmen, die mit dem Server Manager am Secure Server (VPN Gateway) konfiguriert wurden (siehe im Server-Handbuch → LDAP Server)

LdapHost = 127.0.0.1

IP-Adresse des LDAP Hosts im Firmennetz. (Entspricht dem Parameter "LDAP Host" im Server-Handbuch.)

LdapPort = 389

Die Port-Nummer des LDAP Servers. Ändern Sie diesen Wert nur, wenn der LDAP Server definitiv unter einer anderen Port-Nummer als der hier angegebenen Standard-Nummer (389) läuft. (Entspricht dem Parameter "Port |LDAP" im Server-Handbuch.)

LdapAdminDN = cn=xxx,o=xxx,c=xxx

Dieser Distinguished Name (DN) gibt an, wo sich die Konfiguration für den Administrator auf dem LDAP Server befindet. (Entspricht dem Parameter "Administrator DN" im Server-Handbuch.)

LdapPassword	= xxx	Das Passwort des Administrators, um auf den LDAP Server zugreifen zu können. (Entspricht dem Parameter “Administrator Passwort [LDAP” im Server-Handbuch.)
LdapBaseDN	= cn=xxx,o=xxx,c=xx	LDAP-Suchpfad, unterhalb dessen die Benutzer-spezifischen Konfigurationen der Link-Profiles für die Clients auf dem LDAP Server zu finden sind. Diese Clients greifen über das zugehörige VPN Gateway (siehe oben) auf den Management Server zu. Der Benutzername wird unter der LdapBaseDN als Common Name (cn) gesucht.
LdapAuthAttribute	= ncpUserAuthenticationCode	Wenn der Benutzername gefunden wurde, wird ihm der in diesem Attribut eingetragene Wert als Authentication-Code zugeordnet.
[ClientAuthentication]		
AuthCodeMinLen	= 6	Die Mindestlänge des Authentication Codes. (Standard = 6)
AuthCodeValidDays	= 14	Hiermit wird die Gültigkeitsdauer des Authentication Codes in Tagen ab dessen Erzeugung festgelegt.
AuthCodeMaxErrCnt	= 10	Mit dieser Zahl wird bestimmt, wie oft der Authentication Code fehlerhaft eingegeben werden kann. Ist die angegebene Fehlerzahl erreicht, so kann sich der Client nicht mehr anwählen. Eine Aufhebung der Sperre ist nur über die Management Console möglich.
AuthCodeDisableRest	= 0; Bei Konfigurations-Downloads wird der Authentisierungs Code zurück gesetzt. 1 = ... nicht zurück gesetzt.	

[CONNMAN]

In diesem Abschnitt werden die Parameter zum automatischen Update des Auslands-Telefonbuchs für T-Online eingestellt.

URL	= http://www.t-update.de/securevpn/phb.zip
	URL der Telefonbuch-Datei des Connenction Managers. (Überprüfen Sie diesen Eintrag in der Konfigurationsdatei.)
Interval	= 800000
	Zeitabstand in dem ein neues Auslands-Telefonbuch von T-Online herunter geladen werden soll. Die Zeit beginnt erst zu laufen, nachdem zum ersten Mal ein T-Online-Telefonbuch von einem Client angefordert wurde.
ProxyHost	= xxx.xxx.xxx.xxx
	IP-Adresse des HTTP Proxy Servers, falls nötig.
ProxyPort	= 80; Port des Proxy Servers.
ProxyAuthName	= Benutzername für den Proxy Server
ProxyAuthPwd	= Passwort für den Proxy Server

[CMP]

CmpPort =	829; CMP Listen Port.
	0 = CMP Server disabled
CmpPollTime	= 15; CMP Polling-Intervall in Sekunden
LogLevel	= 0
	CMP Log Level. (Mögliche Werte = 0 - 9) Mit dem Wert wird die Tiefe der Analyseebene für die Log-Datei bestimmt.

[RADIUS]

Enabled	= 1	Der integrierte RADIUS Server des Management Systems wird mit 1 aktiviert, mit 0 deaktiviert.
AuthPort	= 1812	Authentication Port (Standard = 1812, sollte nicht verändert werden)
AccPort	= 1813	Accounting Port (Standard = 1813, sollte nicht verändert werden)
LogLevel	= 0	RADIUS Log Level. (Mögliche Werte = 0 - 9) Mit dem Wert wird die Tiefe der Analyseebene für die Log-Datei bestimmt.

[Log]

Mit dem Wert wird die Tiefe der Analyseebene für die Log-Datei bestimmt. (Mögliche Werte = 0 - 9)

LogLevel	= 0	
SessLogLevel	= 0	
MgmLogLevel	= 0	
ReplLogLevel	= 0	
PackageLogLevel	= 0	
LogPath	= ./log	Der Pfad wird mit dem Directory für die Log-Dateien angegeben.

Anzahl der Tage, bis die Log-Einträge gelöscht werden:

LogLifetimeSecurity	= 90
LogLifetimeConfig	= 90
LogLifetimeLogins	= 90
LogLifetimeAdmin	
Logins	= 90
LogLifetimeSystem	= 30
LogLifetimeTasks	= 90
LogLifetimeTrace	= 2
LogLifetimeAccounting	= 90
LogLifetimeSyslog	= 90
LogLifetimeRadius	= 90

[Syslog]

Hosts	= 127.0.0.1; Syslog Server Hostname
Port	= 514; Syslog Destination Port (Standard = 514)
Facility	= 20000; Facility Base
LogTrace	= 0; Facility Base + 1
LogConfig	= 0; Facility Base + 2
LogSecurity	= 0; Facility Base + 3
LogLogins	= 0; Facility Base + 4
LogAdminLogins	= 0; Facility Base + 5
LogSystem	= 0; Facility Base + 6
LogRadius	= 0; Facility Base + 7
ListenPort	= 0; Standard = 514 0 = Listening disabled

[Console]

Console	= 0; aus
Console	= 1; an

2.2.5 Update des Update Clients

Ein neuer Update Client wird wie ein Software-Paket am Rechner des Management Servers installiert, indem UpdRWSRSU2xx.exe gestartet wird.

Die neuen Update Client-Dateien werden in der Datenbank des Management Servers im Verzeichnis rwsrsu\v200* abgelegt, unabhängig von der Versions-Nummer.

Ein anschließender Neustart des Management Servers ist nicht nötig.

3. ncpbudgett.exe – Budget-Manager (Verbindungssteuerung/Verbindungsstatistik)

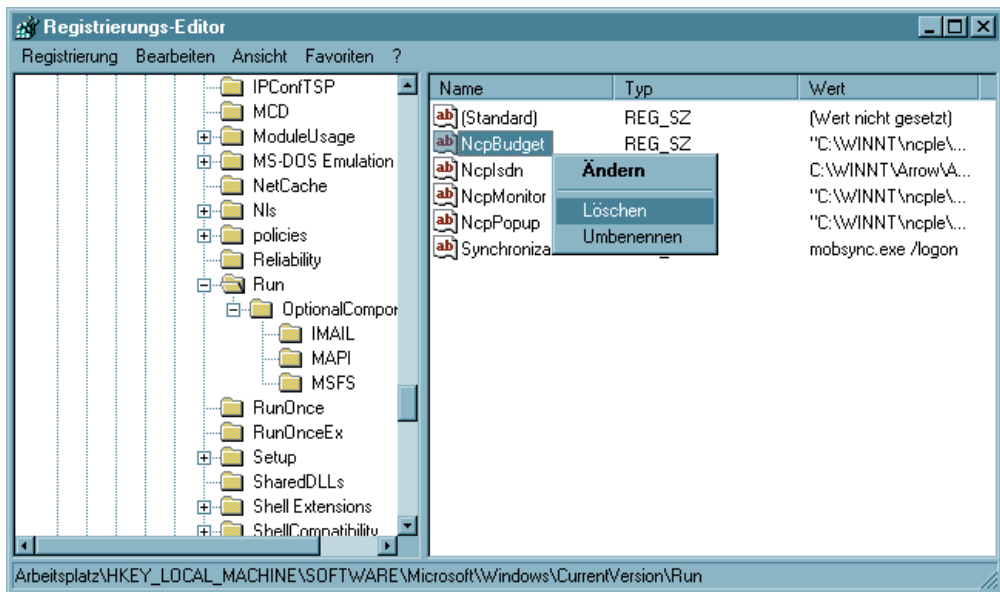
Nach der Installation der Client Software läuft der sogenannte Budget-Manager für Verbindungssteuerung und -statistik automatisch bei Start des Monitors mit.

Der Budget-Manager hat die Aufgabe, Verbindungen der Client Software nach genau definierten Kriterien zu überwachen.

Diese Kriterien werden im Monitormenü unter “Konfiguration / Verbindungssteuerung” festgelegt. (Siehe auch Handbuch zum Secure Client, Monitor, Verbindungssteuerung)

Die Verbindungssteuerung im Monitormenü zu aktivieren ist nur dann sinnvoll, wenn die Verbindungen nicht zu einem Gateway des Firmennetzes führen oder wenn für die Verbindungen Gebühren für Verbindungszeit oder -häufigkeit anfallen. Ansonsten kann das Gebühren-Management zentral administriert werden.

Wird der Budget-Manager nicht genutzt, so kann er aus der Registry entfernt werden (siehe Bild unten). Dabei ist darauf zu achten, dass er bei einem Update oder einer Neuinstallation automatisch wieder installiert wird. Danach muss er erneut mit regedit gelöscht werden.



Key: `Software\Microsoft\Windows\CurrentVersion\Run\NCPBudget`

4. rws cmd.exe – Kommandozeilen-Schnittstelle



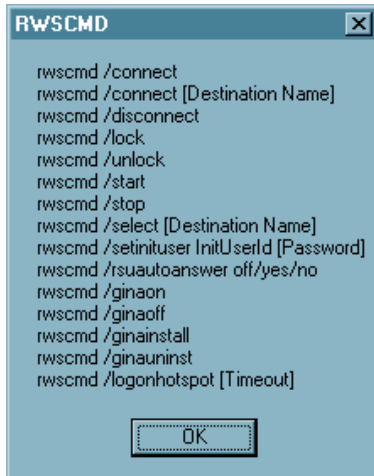
Achtung! Die folgende Beschreibung gilt nur für Windows-Systeme.

4.1 Übergabe von Kommandos an den NCP Secure Client

Der NCP Secure Client (Entry/Enterprise/GovNet Client) verfügt mit rws cmd.exe über eine Kommandozeilen-Schnittstelle, die für andere Anwendungen genutzt werden kann. Voraussetzung für die Nutzung des Programms rws cmd.exe ist eine Client Software, die mindestens den Stand 7.0 (Enterprise Client) bzw. 8.0 (Entry Client) hat.

Bei der Installation wird der Kommandozeileninterpreter in das ncple-Verzeichnis unter Windows kopiert. Der Aufruf erfolgt aus diesem Verzeichnis (z.B.):

```
C:\Windows\ncple>rws cmd /<Kommando>
```



Wird die Syntax beim Aufruf nicht eingehalten oder ein Kommando falsch oder unvollständig angegeben, so erscheint ein Fenster, in dem die möglichen Kommandos aufgelistet sind:

```
connect
connect [Destination Name]
disconnect
lock
unlock
start
stop
select [Destination Name]
setinituser InitUserId [Password]
rsuautoanswer off/yes/no
ginaon
ginaoff
ginainstall
ginaunins
logonhotspot [Timeout]
```

4.2 Voraussetzung für die Nutzung des Programms

- Die Dienste ncprwsnt, ncpsec und rwsrsu müssen gestartet sein. Diese Dienste werden nach der Installation der Client Software standardmäßig gestartet – sie befinden sich im Verzeichnis
C:\Windows\ncple>
- Der Monitor muss nur gestartet werden, wenn Passwörter oder Pin-Eingaben erforderlich sind, da rwsrmd.exe keinen PIN-Dialog startet.
- Weiterhin müssen Schreibrechte bestehen auf den Registrykey:
KEY_LOCAL_MACHINE\
Software\NCP engineering GmbH\NCP Enterprise Monitor

4.3 Beschreibung der Kommandos

`rwsrmd /connect`

Erforderliche Windows Berechtigung: User Rechte

Beschreibung: Verbindungsaufbau mit dem zuletzt im Monitor gesetzten Zieleintrag.

`connect [Destination Name]`

z.B.: `rwsrmd /connect "LAN via Router (IP)"`

Erforderliche Windows Berechtigung: User Rechte

Beschreibung: Verbindungsaufbau mit dem übergebenen Zieleintrag.



Die Hochkommas werden statt der eckigen Klammern gesetzt. Sie sind notwendig, da es sich um eine Übergabe mit Leerzeichen handelt.

`rwsrmd /disconnect`

Erforderliche Windows Berechtigung: User Rechte

Beschreibung: Trennt die aktuelle Verbindung.

`rwsrmd /lock`

Erforderliche Windows Berechtigung: User Rechte

Beschreibung: Sperrt den Client, kein Verbindungsaufbau mehr möglich

```
rwscmd /unlock
```

Erforderliche Windows Berechtigung: User Rechte

Beschreibung: Entsperrt den Client, setzt die durch Lock gesetzte Sperre zurück

```
rwscmd /start
```

Erforderliche Windows Berechtigung: Administrator Rechte

Beschreibung: Startet alle Dienste, Popup und Monitor des NCP Secure Clients

Bei erneutem Aufruf kommt der Hinweis "Secure Client ist bereits geöffnet".

```
rwscmd /stop
```

Erforderliche Windows Berechtigung: Administrator Rechte

Beschreibung: Stoppt alle Dienste und den Monitor des NCP Secure Clients

Zu beachten ist außerdem, dass, wenn das Kommando `rwscmd /stop` ausgeführt wurde, danach das Kommando `rwscmd /start` ausgeführt werden muss, damit die Dienste und der Monitor wieder gestartet werden. Ein Reboot genügt in diesem Fall nicht, da das Popup und der Monitor nicht gestartet werden.

```
rwscmd /select "Destination Name"
```

Erforderliche Windows Berechtigung: User Rechte

Beschreibung: Im Secure Client wird auf das gewünschten Ziel gewechselt.



Die Hochkommas werden statt der eckigen Klammern gesetzt. Sie sind notwendig, da es sich um eine Übergabe mit Leerzeichen handelt.

```
rwscmd /setinituser UserId "Passwort"
```

Erforderliche Windows Berechtigung: Administrator Rechte

Beschreibung: Soll kein Fenster bei der Initialverbindung angezeigt werden, kann die User Id des Benutzers für die Erstanmeldung und optional das Passwort für den Initprozess übergeben werden.



Die Hochkommas werden statt der eckigen Klammern gesetzt. Sie sind notwendig, da es sich um eine Übergabe mit Leerzeichen handelt.

```
rwscmd /rsuautoanswer off/yes/no
```

Erforderliche Windows Berechtigung: Administrator Rechte

Beschreibung: Hier wird eingestellt, wie bei Anfragen nach einem Softwareupdate reagiert wird.

yes	Client Software erhält automatisch ohne Nachfrage ein Update.
no	automatisches Software Update wird abgelehnt und nicht ausgeführt.
off	Bei der Einstellung off wird in einem Meldungsfenster nachgefragt, ob die Software aktualisiert werden soll.

```
rwscmd /ginainstall
```

Erforderliche Windows Berechtigung: Administrator Rechte

Beschreibung: Installiert die NCP Gina, sofern dies noch nicht bei der Software-Installation geschehen ist (vergleiche im Client-Handbuch den Abschnitt "Installation").

```
rwscmd /ginaunins
```

Erforderliche Windows Berechtigung: Administrator Rechte

Beschreibung: Deinstalliert die NCP Gina. Sollte die NCP Gina von einer fremden Gina aufgerufen werden, so ist die Deinstallation mit diesem Kommando nicht möglich. In diesem Fall muss die Entfernung aus der Registry manuell vorgenommen werden, oder die Ginas in umgekehrter Reihenfolge der Installation wieder deinstalliert werden (vergleiche im Client-Handbuch den Abschnitt "Logon Optionen").

```
rwscmd /ginaon
```

Erforderliche Windows Berechtigung: Administrator Rechte

Beschreibung: Schaltet die NCP Gina-Dialoge zur Anmeldung an das VPN Gateway sichtbar, sofern die NCP Gina installiert wurde.

```
rwscmd /ginaoff
```

Erforderliche Windows Berechtigung: Administrator Rechte

Beschreibung: Schaltet die NCP Gina-Dialoge unsichtbar und überspringt damit die VPN Gateway-Anmeldung mit der NCP Gina.

```
rwscmd /logonhotspot [Timeout]
```

Soll über einen externen Dialer eine Hotspot-Anmeldung erfolgen, kann mit diesem Befehl die Firewall für die Ports 80 (HTTP) und 443 (HTTPS) freigeschaltet werden. Damit wird eine dynamische Regel erzeugt, die den Datenverkehr zulässt, bis der übergebene Timeout (in Sekunden) abgelaufen ist.



Weil damit über die Kommandozeile die Firewall freigeschaltet werden kann, wurde in den Firewall-Einstellungen unter "Optionen" der Parameter "Hotspot-Anmeldung für externe Dialer zulassen" hinzugefügt. Erst wenn dieser aktiviert ist, kann der Befehl über `rwscmd` ausgeführt werden. (Siehe dazu -> Konfigurationsparameter / Telefonbuch, Firewall-Einstellungen).

5. ncprwsnt.exe

Zuständig für das Frame Processing der Datenkommunikation über NCP PPP und VPN, sowie die Wähldienste.

Mit diesem Dienst können automatisch Anwendungen nach einem Verbindungsauf- oder -abbau gestartet werden, die Systemrechte benötigen. Dazu müssen im Installationsverzeichnis zwei Batch-Dateien editiert werden:

connect.bat

In der Batch-Datei mit genau dieser Schreibweise werden die ausführbaren Programme oder Batch-Dateien eingetragen, die nach einem Verbindungsaufbau ausgeführt werden sollen.

disconnect.bat

In der Batch-Datei mit genau dieser Schreibweise werden die ausführbaren Programme oder Batch-Dateien eingetragen, die nach einem Verbindungsabbau ausgeführt werden sollen.



Beachten Sie dazu auch den Parameter "Ausführung von "(dis)connect.bat" nicht zulassen". Er befindet sich im Monitormenü "Verbindungssteuerung / Ext. Anwendungen" unter dem Menüpunkt "Konfiguration".



Diese Funktion sollte immer aktiviert sein, wenn nicht unbedingt für eine gewünschte Anwendung die Ausführung der genannten Batch-Dateien mit Administrator-Rechten erforderlich ist.

Die Anwendungen (Batch-Dateien) für deren Ausführung Benutzerrechte genügen, können aus eben diesem Monitormenü "Konfiguration / Verbindungssteuerung/ Ext. Anwendungen" gestartet werden, indem sie dort direkt eingetragen werden (siehe → Client-Monitor / Verbindungssteuerung).